AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Kibertəhlükəsizlik
Təşkilatları Assosiasiyası

Şəbəkə təhlükəsizliyi

fənni üzrə mühazirələr toplusu

Aidə Mustafayeva

Bu vəsait Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən "İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərinin hazırlanması" layihəsi çərçivəsində hazırlanmışdır.

AZƏRBAYCAN KİBERTƏHLÜKƏSİZLİK TƏŞKİLATLARI ASSOSİASİYASI
MİNGƏÇEVİR DÖVLƏT UNİVERSİTETİ

Müəllif:
Aidə Mustafayeva. Şəbəkə təhlükəzisliyi. Dərslik, 2024

Bu vəsait Azərbaycan Repsublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən "İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərin hazırlanması" layihəsi çərçivəsində hazırlanmışdır. Nəşrin məzmununa görə donor məsuliyyət daşımır.

Kitab Azərbaycan Kiber Təhlükəsizlik Təşkilatları Assosiasiyası və Mingəçevir Dövlət Universitetinin təşkilatçılığı ilə ərsəyə gəlmişdir. Şəbəkə təhlükəsizliyi üzrə tədris materialının hazırlanmasında əsas məqsəd şəbəkə təhlükəsizliyi sahəsində işləmək üçün lazımi bilik və bacarıqların verilməsini nəzərdə tutmaqla, təhsilalanlara kibertəhlükəsizlik sahəsində məlumatlılığının artırılmasını təmin etməkdir. Hər bir modul əsas prinsiplərdən tutmuş şəbəkənin idarə edilməsi, autentifikasiya, avtorizasiya və audit kimi daha ixtisaslaşmış mövzulara, həmçinin ümumi təhdidlər və zəifliklərə qədər şəbəkə təhlükəsizliyinin əsas aspektlərini əhatə edir. Tədris vəsaitində tələbələrə təkcə nəzəri biliklər vermək deyil, həm də keys tədqiqatları və digər interaktiv tədris metodları vasitəsilə praktiki bacarıqların formalaşdırılmasına dəstək olmaqdır. Bu, tələbələrə biliklərini real həyat vəziyyətlərində səmərəli şəkildə tətbiq etmək üçün lazımi vasitələrlə təmin edəcəkdir.
Əminik ki, bu kitab tələbələr, müəllimlər və şəbəkə təhlükəsizliyi sahəsində daha çox anlayış və bacarıq əldə etməkdə maraqlı olan hər kəs üçün dəyərli mənbə olacaqdır.

Şəbəkə təhlükəsizliyi.
DƏRSLİK
BAKI, AKTA, MDU, 2024.

GİRİŞ

IV və V sənaye texnologiyalarının tətbiqilə inkişaf etmiş cəmiyyətimizin elə ən güclü və ən zəif tərəflərini də məhz rəqəmsal resurslar təşkil edir. Belə ki, bu texnologiyalardan istifadə etməklə inkişaf edən cəmiyyətimizin güclü tərəfi – dayanıqlığı, davamlığı, dəqiqliyi, çevikliyi və sürətliliyi təmin edən SMART texnologiyaların tətbiqi ilə bağlıdırsa, eyni zamanda fəaliyyət infrastrukturlarında bu texnologiyaların tətbiqinin sürətlənməsi yarana biləcək təhlükələrin artmasına səbəb olurki, bu da kiberhücumlar və məlumat sızması risklərinin artması ilə həmin rəqəmsal resursların zəif tərəflərini önə çıxardır. Fəaliyyət sektorlarında təbii, texnogen və ya qəsdən törədilən təhlükələr resursların təchizatı və ya kritik xidmətlərin fəaliyyəti üçün ciddi problemlərin yaranmasına səbəb olur. Kiber təhdidlərin və texnologiyanın inkişafının sürətli və davamlı inkişafı ilə daha çox təşkilat və fərd öz şəbəkələrinin və məlumatlarının təhlükəsizliyi və qorunması ilə bağlı risklərlə üzləşir. Kiberhücumlar, viruslar, fişinq, DDoS hücumları və digər təhdid növləri onlayn təhlükəsizlik üçün ciddi problemlər yaradır. Şəbəkələrdə ötürülən və saxlanılan məlumatların həcminin artması, eləcə də Əşyaların İnternetinin (IoT) inkişafı ilə şəbəkə infrastrukturunda zəif nöqtələr daha da kritik xarakter alır. Uğurlu kiberhücumlar ciddi maliyyə itkilərinə, məxfi məlumatların sızmasına və müştərilərin etibarının pozulmasına səbəb ola bilər. Buna görə də, şəbəkə təhlükəsizliyi məsələləri bütün ölçülü təşkilatlardan daimi diqqət və investisiya tələb edir. Hücumların aşkarlanması və qarşısının alınması üçün yeni üsul və vasitələrin inkişafı, işçilərin təlimi və təhlükəsizlik sistemlərinin mütəmadi olaraq yenilənməsi rəqəmsal dünyada təhlükəsizliyi qorumaq üçün zərurətə çevrilir. Məhz bu baxımdan şəbəkə təhlükəsizliyi üzrə dərs vəsaitinin hazırlanması məqsədəuyğundur.

"Şəbəkə təhlükəsizliyi" dərs vəsaiti rəqəmsal kiber məkanda informasiya təhlükəsizliyini və məlumatların bütövlüyünü təmin etmək istəyən hər kəs üçün əvəzolunmaz mənbəyə çevriləcəkdir. Kitab bu sahədə biliklərini dərinləşdirmək istəyənlər üçün əsl bələdçidir. O, şəbəkə təhlükəsizliyinin əsas prinsiplərini başa düşmək üçün istifadəçilərə əsas anlayışlardan tutmuş təhdidlərdən daha mürəkkəb qorunma üsullarına qədər bütün sahələri əhatə edir.

Dərslik 050615 – "İnformasiya təhlükəsizliyi" ixtisası üzrə Təhsil proqramının ixtisas fənn blokuna daxil edilmiş "Şəbəkələrin təhlükəsizliyi (Network Security)" fənninin işçi tədris proqramına və Azərbaycan

Respublikası Elm və Təhsil Nazirliyinin 11 sentyabr 2008-ci il tarixli 1060 №li əmri ilə təsdiq edilmiş "Kredit sistemi ilə təhsil alan tələbələrin biliyinin qiymətləndirilməsi haqqında", Nazirlər Kabinetinin 23 aprel 2010- cu il tarixli 75 saylı qərarı ilə təsdiq edilmiş "Ali Təhsil pilləsinin Dövlət Standartı və proqramı" 050615 – "İnformasiya təhlükəsizliyi" ixtisası isə 28.07.2022-ci il tarixli F-463 №li əmri ilə təsdiq edilmiş "Bakalavriat səviyyəsinin (əsas (baza) Ali Tibb Təhsilinin)" ixtisas üzrə təhsil proqramının tələblərinə uyğun hazırlanmışdır.

Təhsil proqramında fənnin tədris mövzuları haqqında aşağıdakılar qeyd olunmuşdur: fənn çərçivəsində şəbəkələrin təhlükəsizlik məsələləri anlaşılsın deyə şəbəkələr barədə daha dərin biliklər öyrədilir. Tələbələr burada RADIUS, TACACS+, Kerberos, SSO, LDAP və s. kimi anlayışlar bilməli və fərqli şəbəkə avadanlıqları (IDS, IPS) barədə biliklər əldə etməlidir. Şəbəkələrin auditini ve loqlaşdırmasını öyrənir. Şəbəkələrdə sniffing mexanizmlərini, şəbəkələrdə təhlükəsizliyin təmin olunması üçün lazım olan sazlamalar barədə öyrənir. Şəbəkədə mövcud təhlükəsizlik protokollarının anlayır və istifadə edir. Yeni nəsil təhlükəsizlik divarları eləcə də, SIEM, SOAR, UEBA barədə məlumatları öyrənir. Şəbəkələrin auditini ve loqlaşdırmasını, şəbəkələrdə sniffing mexanizmlərini, şəbəkələrdə təhlükəsizliyin təmin olunması üçün lazım olan sazlamaları, Yeni nəsil təhlükəsizlik divarlarının yaradılmasını, eləcə də, SIEM, SOAR, UEBA barədə məlumatları öyrənir. Şəbəkədə mövcud təhlükəsizlik protokollarını anlayır və istifadə edir.

Kitab 10 moduldan ibarətdirdir. Hər modul təhlükəsizliyin təmin olunmasında tələb olunan bilik və bacarıqların əldə olunmasına dəstək olacaqdır.

MODUL 1. TƏHLÜKƏSİZLİYİN ƏSASLARI

Modul 1 təhlükəsizliyin əsaslarını, o cümlədən təhlükəsizliyə girişi, təhlükəsizliyin növləri və standartlarını və bu sahəni anlamaq üçün lazım olan əsas anlayışları və terminləri əhatə edir. İnformasiyanın mühafizəsinin təmin edilməsi məsələlərinə məxfilik, bütövlük və əlçatanlıq daxil olmaqla, informasiya təhlükəsizliyinin üçlü modeli əsasında baxılır. Effektiv təhlükəsizlik tədbirlərinin hazırlanması və həyata keçirilməsi üçün əsas olan təhlükəsizlik prinsiplərinə xüsusi diqqət yetirilir.

Əldə olunan kompetensiyalar:

-əsas təhlükəsizlik anlayışları və prinsipləri haqqında anlayış əldə edir.

-təhdidləri necə tanıyıb təsnif etməyi öyrənir.

-beynəlxalq təhlükəsizlik standartlarına və modellərinə uyğun olaraq riskləri qiymətləndirə və müvafiq qoruyucu tədbirləri tətbiq edə bilirlər.

MODUL 2. ŞƏBƏKƏ CİHAZLARI VƏ TEXNOLOGİYALARI

Modul şəbəkə qurğuları və texnologiyalarının öyrənilməsinə həsr olunub. Aktiv və passiv şəbəkə cihazları, həmçinin əsas OSI və TCP/IP şəbəkə modelləri əhatə olunur. Port nömrələri və şəbəkə protokolları, o cümlədən İnternet səviyyəsinin IPv4 və IPv6 protokolları öyrənilir. Müasir şəbəkə infrastrukturunda mühüm rol oynayan şəbəkə problemlərinin aradan qaldırılması və virtuallaşdırma texnologiyalarına ətraflı diqqət yetirilir və aradan qaldırılması, şəbəkə virtualizasiyası üsulları nəzərdən keçirilir.

Əldə olunan kompetensiyalar:

- şəbəkə qurğularının iş prinsipləri haqqında biliklərə yiyələnir,

- şəbəkə modellərinin və protokollarının əsaslarını başa düşür, həmçinin şəbəkə nasazlıqlarının diaqnostikası və aradan qaldırılması bacarıqlarını inkişaf etdirirlər.

- virtuallaşdırma texnologiyaları ilə də tanış olurlar ki, bu da onlara şəbəkə infrastrukturunu optimallaşdırmaq üçün bu texnologiyalardan istifadə etməyə imkan verir.

MODUL 3. ŞƏBƏKƏ TOPOLOGİYASI

Modul şəbəkə topologiyalarının və onların dizaynının öyrənilməsinə həsr edilmişdir. Ulduz, şin, halqa və onların hibrid formaları kimi müxtəlif topologiya növləri nəzərdən keçirilir. Diqqət şəbəkənin etibarlılığının təmin edilməsində mühüm aspekt olan fiziki əlaqə problemlərinin aradan qaldırılmasına yönəlib. Şəbəkə infrastrukturunun səmərəli təşkili üçün istifadə olunan Ethernet standartları və naqillərin paylanması texnologiyaları öyrənilir.

Əldə olunan kompetensiyalar:

- şəbəkələrin və topologiyaların layihələndirilməsi prinsipləri haqqında biliklər əldə edir.

- fiziki birləşmələrlə bağlı problemlərin diaqnostikası və aradan qaldırılması bacarıqlarını inkişaf etdirirlər.

- Ethernet standartları ilə tanış olur və səmərəli şəbəkə həlləri yaratmaq üçün naqil paylama texnologiyalarından istifadə etmək bacarığı qazanırlar.

MODUL 4. ŞƏBƏKƏNİN İDARƏ EDİLMƏSİ

Modul şəbəkə idarəçiliyinə diqqət yetirir və effektiv şəbəkə idarəetməsi üçün lazım olan əsas prinsipləri əhatə edir. Modul mərkəzləşdirilmiş sistemlərdən paylanmış sistemlərə qədər müxtəlif şəbəkə idarəetmə arxitekturalarını araşdırır. Şəbəkə idarəetmə sisteminin əsas komponentlərinə, məsələn, monitorinq cihazları, şəbəkənin konfiqurasiyası və saxlanması üçün alətlər və şəbəkə təhlükəsizliyini və performansını təmin etmək üsullarına diqqət yetirir. Şəbəkənin idarə edilməsi üçün əsas protokol olan SNMP-yə (Simple Network Management Protocol) xüsusi diqqət yetirilir. SNMP-ni öyrənmək onun şəbəkə sağlamlığının monitorinqi, cihazın idarə edilməsi və performans məlumatlarının toplanması kimi funksionallığını başa düşməyi əhatə edir. Modul həmçinin şəbəkə infrastrukturunun dəstəklənməsi və inkişafında mühüm rol oynayan sistem və şəbəkə proqram təminatı məsələlərini də əhatə edir. Bu proqramlar tapşırıqların avtomatlaşdırılması, məlumatların təhlili və konfiqurasiyanın idarə edilməsini təmin edir. Bundan əlavə, modul şəbəkənin idarə olunması prosesində şəffaflığın və təşkilatçılığın qorunması üçün zəruri olan şəbəkə sənədlərinin yoxlanılmasını əhatə edir. Şəbəkə sənədlərinə şəbəkə planları, məftil diaqramları, performans hesabatları və konfiqurasiya məlumatları daxil ola bilər. Bu sənədlərin başa düşülməsi və saxlanması daha səmərəli idarəetməni asanlaşdırır və problemlərin aradan qaldırılması prosesini sürətləndirir.

Əldə olunan kompetensiyalar:

- şəbəkənin idarə edilməsi, o cümlədən şəbəkə qurğularının və proqram təminatının qurulması, monitorinqi və dəstəklənməsi bacarıqları əldə edirlər.
- şəbəkənin davamlılığını, dayanıqlığını və təhlükəsizliyini qorumaq üçün vacib olan şəbəkə proseslərini sənədləşdirmək bacarığını inkişaf etdirirlər.
- SNMP və Syslog protokolları və onların şəbəkə idarəetməsində tətbiqi haqqında biliklər.
- şəbəkə trafikini təhlil etmək və performans problemlərini müəyyən etmək bacarığı.
- şəbəkə sənədlərinin yaradılması və saxlanması üzrə bacarıqlar.
- QoS anlayışını və onun şəbəkə performansının optimallaşdırılmasındakı rolunu başa düşmək.

MODUL 5. ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNƏ GİRİŞ

Modul şəbəkə infrastrukturunun qorunmasının əsas aspektlərini əhatə edən şəbəkə təhlükəsizliyinə giriş təqdim edir. Şəbəkə təhlükəsizliyinin əsas məqsədi məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək və icazəsiz girişin qarşısını almaqdır. Şəbəkə təhlükəsizliyi mövzusunun öyrənilməsi monitorinq, təhlükənin qarşısının alınması və insidentlərə reaksiya kimi şəbəkə təhlükəsizliyi üzrə mütəxəssislərin məsuliyyətlərini dərk etməkdən ibarətdir. Şəbəkə təhlükəsizliyinin müxtəlif növləri, o cümlədən fiziki, proqram təminatı və təşkilati müdafiə nəzərdə tutulur. Fiziki təhlükəsizlik avadanlıqlara giriş nəzarətini əhatə edir, proqram təminatı isə antivirusların, firewallların və müdaxilənin aşkarlanması sistemlərinin istifadəsini əhatə edir. Təşkilati təhlükəsizlik nəzarətləri ümumi şəbəkə təhlükəsizliyini yaxşılaşdırmağa kömək edən siyasət və prosedurlar yaradır. Modul həmçinin həm aparat, həm də proqram təminatı həllərini özündə birləşdirən şəbəkə təhlükəsizliyi alətlərini araşdırır. Bu alətlər şəbəkənizi DDoS, fişinq və zərərli proqram hücumları kimi hücumlardan qorumaq məqsədi daşıyır. Mühüm cəhət peşəkar səriştənin sübutu olan CISSP, CEH və CompTIA Security+ kimi müasir şəbəkə təhlükəsizliyi sertifikatlarını başa düşməkdir. İT infrastrukturunun yaradılması prinsipləri xarici və daxili təhlükələrə tab gətirə bilən etibarlı və təhlükəsiz şəbəkə mühitinin təmin edilməsi ilə bağlıdır. Şəbəkə perimetri təhlükəsizliyi metodologiyası şəbəkə kənarını xarici təhlükələrdən qoruyan firewall, VPN və müdaxilə aşkarlama sistemlərinin qurulması kimi praktik addımları əhatə edir.

Əldə olunan kompetensiyalar:

- şəbəkə təhlükəsizliyinin məqsədlərini, məsuliyyətlərini və növlərini anlamaq.
- şəbəkə təhlükəsizliyinin əsas aspektləri, o cümlədən təhdid növləri və mühafizə vasitələri haqqında dərin biliklərə yiyələnir.
- etibarlı İT infrastrukturunun yaradılması prinsiplərini və şəbəkə perimetrinin mühafizəsi metodologiyasını başa düşürlər.
- müasir təhlükəsizlik alətləri və texnologiyaları üzrə bacarıqları inkişaf etdiri.
- aparıcı şəbəkə təhlükəsizliyi sertifikatları haqqında anlayış əldə edirlər.

MODUL 6. SİMSİZ (Wİ-Fİ) ŞƏBƏKƏ TƏHLÜKƏSZİLİYİ

Modul Wi-Fi texnologiyasına diqqət yetirməklə simsiz şəbəkələrdə təhlükəsizlik məsələlərini əhatə edir. Modul simsiz texnologiyanın əsaslarını, o cümlədən məlumatların hava ilə ötürülməsi prinsiplərini və radiotezlik spektrindən istifadəni əhatə etməklə başlayır. Simsiz şəbəkələrin giriş nöqtələri, marşrutlaşdırıcılar və müştəri cihazları kimi əsas komponentləri, həmçinin Wi-Fi şəbəkələrinin işləməsini təmin edən IEEE 802.11 kimi əsas protokollar öyrənilir. Simsiz şəbəkələrdə məlumatların qorunmasında mühüm rol oynayan kriptoqrafiya və şifrələmə protokollarına xüsusi diqqət yetirilir. Modul WEP, WPA, WPA2 və WPA3 kimi təhlükəsizlik protokollarını, o cümlədən onların zəifliklərı və üstünlüklərini təhlil edir. Şəbəkəyə icazəsiz girişin qarşısını almaq və məxfi məlumatları qorumaq üçün etibarlı şifrələmə ehtiyacına diqqət yetirilir. MAC ünvanının filtrlənməsi yalnız müəyyən cihazlara şəbəkəyə girişi məhdudlaşdırmaq üçün əlavə təhlükəsizlik üsulu kimi təqdim olunur. Modul həmçinin simsiz cihazların yerləşdirilməsi və siqnal gücünün tənzimlənməsi qaydaları ilə bağlı məsələləri həll edir ki, bu da məlumatların tutulması riskini minimuma endirmək və şəbəkə sabitliyini yaxşılaşdırmaq üçün vacibdir.

Əldə olunan kompetensiyalar:

- simsiz texnologiyanın prinsipləri və əsas protokollar haqqında biliklərə yiyələnir.
- kriptoqrafiyanın əhəmiyyətini başa düşür və məlumatların qorunması üçün müxtəlif şifrələmə üsullarını tətbiq edə bilirlər.
- maksimum şəbəkə təhlükəsizliyini və performansını təmin etmək üçün MAC ünvanlarının filtrasiyası və cihazın düzgün yerləşdirilməsi bacarıqlarını inkişaf etdirirlər.

MODUL 7. AUTENTİFİKASİYA, AVTORİZASİYA VƏ ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ

Modul AAA (Authentication, Authorization, Accounting) konsepsiyası kimi tanınan autentifikasiya, avtorizasiya və auditlə bağlı şəbəkə təhlükəsizliyinin əsas aspektlərini əhatə edir. AAA təhlükəsizliyi konsepsiyasına giriş identifikasiya, avtorizasiya və uçot proseslərinin şəbəkə resurslarının qorunmasında necə mühüm rol oynadığını anlamağa kömək edir. İdentifikasiya şəbəkəyə giriş icazəsi verməzdən əvvəl istifadəçi və ya cihazın

şəxsiyyətini təsdiqləmək üçün yoxlamanı əhatə edir. Təhlükəsizlik səviyyəsinin artırılmasına yönəlmiş parolların, birdəfəlik kodların, biometriklərin və digər yoxlama vasitələrinin istifadəsi də daxil olmaqla, müxtəlif autentifikasiya üsulları nəzərdən keçirilir. Parolun təhlükəsizliyi vacib bir məsələdir və modul güclü parolların necə yaradılacağını və idarə olunacağını və onların təhlükədən necə qorunacağını araşdırır. Avtorizasiya giriş nəzarəti ilə bağlıdır və DAC (İstəyən Giriş Nəzarəti), MAC (Məcburi Giriş Nəzarəti) və RBAC (Rol əsaslı Giriş Nəzarəti) kimi girişə nəzarət modellərinin istifadəsini nəzərdə tutur. Bu modellər istifadəçilərin sistemdəki rollarına və imtiyazlarına əsasən hansı resursların və fəaliyyətlərin mövcud olduğuna nəzarəti təmin edir. AAA konsepsiyasının mühüm elementi olan şəbəkə təhlükəsizliyi auditi şəbəkədə baş verən hadisələrin monitorinqi, təhlili və sənədləşdirilməsi prosesini əhatə edir. Şəbəkə təhlükəsizliyi auditi alətləri zəiflikləri müəyyən etməyə, istifadəçi fəaliyyətinə nəzarət etməyə və təhlükəsizlik siyasətlərinə uyğunluğu təmin etməyə kömək edir. Modul həmçinin müdaxilənin aşkarlanması və qarşısının alınması sistemləri, hadisə qeydləri və şəbəkə trafikinin təhlili alətləri kimi müxtəlif audit alətlərini əhatə edir.

Əldə olunan kompetensiyalar:

-autentifikasiya üsulları, girişə nəzarət modelləri və şəbəkə təhlükəsizliyinin audit prosesi daxil olmaqla AAA konsepsiyaları haqqında dərin bilik əldə edəcəklər.

-şəbəkə resurslarını effektiv şəkildə qorumağa və müəyyən edilmiş standartlara uyğun olaraq təhlükəsizliyini təmin etməyə imkan verən girişə nəzarət və hadisələrin təhlili bacarıqlarını inkişaf etdirirlər.

MODUL 8. ÜMUMİ TƏHDİDLƏR VƏ ZƏİFLİKLƏR

Modul 8 məlumat məxfiliyinə, bütövlüyünə və əlçatanlığına diqqət yetirməklə, şəbəkə təhlükəsizliyinə təsir edən ümumi təhdidlər və zəifliklərə diqqət yetirir. Modul icazəsiz məlumat əldə etmək, məlumat sızıntıları və həssas məlumatların qorunmasını poza biləcək casusluq kimi əsas məxfilik təhdidlərini həll edir. Dürüstlük təhdidləri məlumatların dəyişdirilməsi və ya korlanması ilə əlaqədardır ki, bu da onların dəqiqliyini və etibarlılığını poza bilər. Resursları istifadəçilər üçün əlçatmaz edə bilən DDoS kimi hücumlar zamanı məlumatların əlçatanlığı risk altındadır. Modulda mühüm yer Wi-Fi şəbəkələrinin zəif tərəflərinin, o cümlədən şifrələmə protokollarındakı boşluqlar, səhv təhlükəsizlik parametrləri və köhnəlmiş autentifikasiya

metodlarından istifadə nəticəsində yaranan təhdidlərin təhlilinə verilir. Routerlər, açarlar və giriş nöqtələri kimi şəbəkə cihazlarının zəif tərəflərini başa düşmək də vacib aspektdir, çünki onların səhv konfiqurasiyası və ya yeniləmələrinin olmaması hücumlar üçün giriş nöqtəsinə çevrilə bilər. Modul həm insan faktorları, həm də texniki zəifliklər nəticəsində yarana biləcək təhlükəsizlik təhdidləri və riskləri ilə bağlı məsələləri həll edir. Fişinq, məlumatların ələ keçirilməsi və zərərli proqram hücumları kimi hücum ssenariləri, eləcə də güclü təhlükəsizlik tədbirləri və müntəzəm şəbəkə monitorinqi həyata keçirməklə bu risklərin azaldılması üsulları əhatə olunur.

Əldə olunan kompetensiyalar:

- şəbəkələrin təhlükəsizliyinə təsir edə biləcək müxtəlif növ təhlükələr və zəifliklər haqqında biliklər əldə edirlər.

- risk təhlili bacarıqlarını və məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını necə qorumaq barədə anlayışı inkişaf etdirir.

- şəbəkə infrastrukturunun zəif tərəflərini müəyyən etmək və cihaz və protokol səviyyəsində hücumların qarşısını almaq bacarıqlarını gücləndirirlər.

MODUL 9. FİREWALL – ŞƏBƏKƏLƏRARASI EKRANLAŞDIRMA

Modul firewallların, onların funksiyalarının və təhlükəsizlik divarının əsas aspektlərinin öyrənilməsinə həsr edilmişdir. Bu modul şəbəkənin icazəsiz girişdən və müxtəlif kiberhücumlardan qorunmasında əsas element olan firewallun əsas aksesuarları və funksiyalarını əhatə edir. Firewall daxili şəbəkə ilə xarici şəbəkələr arasında maneə rolunu oynayır, müəyyən edilmiş təhlükəsizlik qaydaları əsasında daxil olan və gedən trafiki süzür. Filtrləmə qaydalarının qurulması, təhlükəsizlik siyasətlərinin yaradılması və şəbəkə trafikinin monitorinqi daxil olmaqla, əsas firewall konfiqurasiyasını və əməliyyatını öyrənir. Mühüm cəhət, infrastrukturun tələblərindən asılı olaraq müxtəlif səviyyəli qorunma təmin edən şəbəkə, şəxsi və korporativ həllər kimi müxtəlif növ firewallları başa düşməkdir. Modul həmçinin firewallun əsas funksiyası olan paket filtrləmə prosesini də əhatə edir. Paket filtrasiyası sizə paket başlıqlarında olan məlumatlara, məsələn, IP ünvanları və port nömrələri əsasında şəbəkə bağlantılarını bloklamağa və ya icazə verməyə imkan verir. Bu, zərərli məlumatların daxil olmasının qarşısını alır və şəbəkəni hücumlardan qoruyur. Şəbəkə Ünvanının Tərcüməsi (NAT) daxili şəbəkə IP ünvanlarını xarici istifadəçilərdən gizlətmək üçün bir üsul olaraq görülür ki, bu da təhlükəsizliyi artırır. NAT, yerli şəbəkədəki birdən çox cihaza İnternetə daxil olmaq üçün bir

ictimai IP ünvanından istifadə etməyə imkan verir, xüsusi cihazlara xarici hücumların ehtimalını azaldır.

Əldə olunan kompetensiyalar:

- firewallları konfiqurasiya edə və idarə edə, paket filtrasiyasını başa düşə və şəbəkə təhlükəsizliyini yaxşılaşdırmaq üçün NAT-dan istifadə edə biləcəklər.
- şəbəkəni xarici təhdidlərdən qoruyan təhlükəsizlik siyasətlərini yaratmaq və konfiqurasiya etmək bacarığını inkişaf etdirir
- müxtəlif növ firewalllar və onların real dünya ssenarilərində tətbiqləri haqqında anlayışlarını gücləndirirlər.

MODUL 10. İDS/İPS MÜDAXİLƏ SİSTEMLƏRİ

Modul müdaxilənin aşkarlanması və qarşısının alınması sistemlərinə (IDS/IPS) və onların şəbəkə təhlükəsizliyində roluna diqqət yetirir. IDS (Intrusion Detection System) və IPS (Intrusion Prevention System) sistemlərinə giriş onların funksiyalarını və işləmə mexanizmlərini başa düşməyə kömək edir. IDS sistemləri şəbəkə trafikinə nəzarət etmək və haker cəhdi və ya hücumu göstərə biləcək şübhəli fəaliyyət və ya pozuntuları aşkar etmək üçün nəzərdə tutulmuşdur. IDS, məlum hücum imzaları və ya anormal davranış nümunələri əsasında anomaliyaları müəyyən edərək, şəbəkə hadisəsi məlumatlarını toplayır və təhlil edir. IDS-dən fərqli olaraq, IPS sistemləri aktivdir və hücumları aşkar etməklə yanaşı, həm də onların avtomatik qarşısını almağa qadirdir. IPS, IDS ilə eyni aşkarlama metodlarından istifadə edir, lakin əlavə olaraq real vaxtda şübhəli əlaqələri bloklaya və ya məhdudlaşdıra bilər. Modul imza əsaslı, davranış və protokol əsaslı yanaşmalar da daxil olmaqla, bu sistemlərin müxtəlif mexanizmlərini və iş növlərini araşdırır. IDS və IPS arasındakı fərqlərə diqqət yetirərək, onların əlavə xüsusiyyətlərini və insidentlərin idarə edilməsinə yanaşmaları vurğulayır. IDS sistemləri adətən passiv monitorinq rejimində işləyir və şəbəkə trafikinə mane olmur, IPS isə trafiki aktiv şəkildə idarə edir və şəbəkəni qorumaq üçün qabaqlayıcı tədbirlər görür. Modul həmçinin daha dərin təhlil və təhlükəsizliyin idarə edilməsi üçün müxtəlif mənbələrdən hadisə və insident məlumatlarını birləşdirən SIEM (Təhlükəsizlik Məlumatı və Hadisə İdarəetmə) sistemlərinin nəzərdən keçirilməsini əhatə edir. SIEM sistemləri mürəkkəb təhdidləri aşkar etməyə və cavabları əlaqələndirməyə kömək edir. Təhlükəsizlik əməliyyatları mərkəzi (SOC) təşkilat daxilində təhlükəsizlik insidentlərini izləmək və idarə etmək üçün

mərkəzləşdirilmiş yerdir. SOC davamlı görünürlük və təhdidlərə cavab vermək üçün IDS/IPS və SIEM alətlərindən istifadə edir.

Əldə olunan kompetensiyalar:

- müdaxilənin aşkarlanması və qarşısının alınması sistemləri, onların funksionallığı və fərqləri haqqında biliklər əldə edirlər.

- IDS və IPS-nin konfiqurasiyası və idarə edilməsi bacarıqlarını inkişaf etdirir və insidentlərin təhlili və təhlükəsizliyin idarə edilməsi üçün SIEM-dən necə istifadə etməyi başa düşürlər.

- SOC-ların necə işlədiyini və təhlükəsizliyin idarə edilməsində rolunu öyrənirlər.

Bundan əlavə, hər modulun sonunda əldə edilmiş biliklərin möhkəmləndirilməsinə və simsiz şəbəkələrin qurulması və təhlükəsizliyinin təmin edilməsində bacarıqların inkişafına yönəlmiş praktiki tapşırıqlar və nəzərdən keçirmə suallarını əhatə edir.

Ümid edirik ki, bu kitab şəbəkə təhlükəsizliyi ilə maraqlanan hər kəs üçün etibarlı bilik mənbəyinə çevriləcək, onlara müasir kompüter şəbəkələrini daha yaxşı başa düşməyə və daha yaxşı mühafizəsinə kömək edəcəkdir.

Dərs vəsaitinin hazırlanmasında Azərbaycan Respublikası Elm və Təhsil Nazirliyinə, Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyasına dərin təşəkkürümüzü bildiririk.

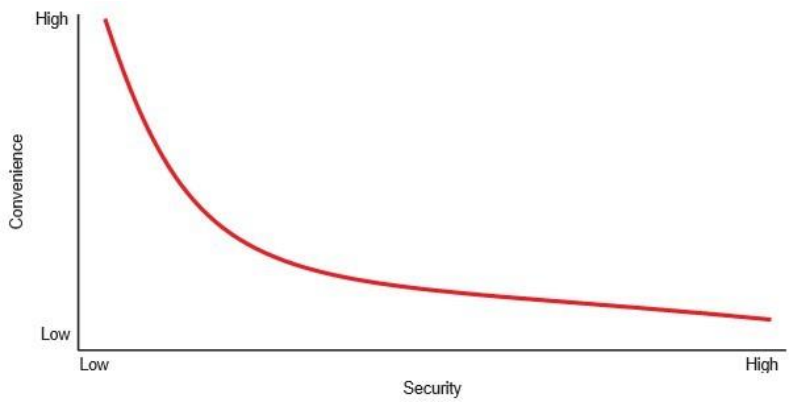
MODUL 1. TƏHLÜKƏSİZLİYİN ƏSASLARI

TƏHLÜKƏSİZLİYƏ GİRİŞ
TƏHLÜKƏSİZLİYİN NÖVLƏRİ VƏ STANDARTLARI
TƏHLÜKƏSİZLİK ANLAYIŞLARI VƏ TERMİNLƏRİ
İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ÜÇLÜ MODELİ
TƏHLÜKƏSİZLİK PRİNSİPLƏRİ

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQLAR

TƏHLÜKƏSİZLİYƏ GİRİŞ

Təhlükəsizlik[1] nədir? Bu söz latın dilindən gəlir və "narahatlıqdan azad" olma mənasını verir. Bəzən təhlükəsizlik, təhlükəsizliyin məqsədi olan təhlükədən azad olma vəziyyəti kimi anlaşılır. O, həm də təhlükəsizliyin təmin edilməsi üçün həyata keçirilən tədbirlər kimi də müəyyən edilir. Tam təhlükəsizliyə heç vaxt nail olmaq mümkün olmadığından, təhlükəsizlik çox vaxt məqsədə deyil, prosesin gedişatına daha çox diqqət yetirir. Bu baxımdan, təhlükəsizlik özümüzü təhlükələrdən qorumaq üçün lazımi addımlar kimi müəyyən edilə bilər. Təhlükəsizlik və rahatlıq arasındakı əlaqə şəkil 1.1-də göstərildiyi kimi tərs mütənasibdir: təhlükəsizlik artdıqca rahatlıq azalır.



Şəkil 1.1. Təhlükəsizlik və rahatlıq arasındakı əlaqə

Təhlükəsizlik və rahatlıq arasında tərs əlaqə ideyası həyatın müxtəlif sahələrində çoxlu nümunələrə malikdir. Ciddi təhlükəsizlik tədbirləri əlverişsiz ola bilər. Təhlükəsizlik səviyyəsi artdıqda, rahatlığı azalda biləcək əlavə qaydalar, prosedurlar və ya məhdudiyyətlər tez-tez tətbiq olunur. Məsələn, hava limanlarında təhlükəsizlik yoxlamalarının artırılması əlavə gecikmələrə və sərnişinlər üçün narahatlıq yarada bilər. Daha sonra fəaliyyət azadlığına məhdudiyyətlər: Daha yüksək səviyyəli təhlükəsizlik çox vaxt daha çox nəzarət və məhdudiyyət tələb edir ki, bu da insanların fəaliyyət azadlığını azalda bilər. Məsələn, ciddi informasiya təhlükəsizliyi qaydaları İnternetdə müəyyən saytlara və ya xidmətlərə girişi məhdudlaşdıra bilər ki, bu da narahatçılığa

[1] Əlizadə M.N., Bayramov H.M., Məmmədov Ə.S. İNFORMASİYA TƏHLÜKƏSİZLİYİ, Dərslik, Bakı, "İQTİSAD UNİVERSİTETİ" nəşriyyatı, şəkilli, 2016 - 384 səh.

səbəb ola bilər. Təhlükəsizliyin artırılması çox vaxt daha az istifadəçi dostu ola biləcək daha mürəkkəb sistemlərin və texnologiyaların tətbiqi deməkdir. Məsələn, biometrik autentifikasiya sistemləri daha təhlükəsiz ola bilər, lakin onların qurulması və istifadəsi sadə parollardan daha çox vaxt və səy tələb edə bilər.

Bəzən təhlükəsizliyin təkmilləşdirilməsi əhəmiyyətli maliyyə xərcləri tələb edir ki, bu da məhsul və ya xidmətin dəyərinin artmasına səbəb ola bilər. Xüsusilə istehlakçılar əlavə təhlükəsizlik üçün daha çox pul ödəməyə hazır deyillərsə, bu da narahatlıq sayıla bilər.

Beləliklə, təkmilləşdirilmiş təhlükəsizlik insanları və məlumatları qorumaq üçün vacib olsa da, bu, çox vaxt rahatlıq və azadlığın azalması ilə başa gəlir.

Məlumdur ki, müasir cəmiyyətdə rəqabətin önündə əsas aktiv kimi informasiyaya təqdim olunan baxış olduqca cəlb edici və aktual görünür. Müasir bilik və texnologiya yönümlü informasiya cəmiyyətində informasiya həm fərdi, həm də kollektiv səviyyədə uğuru şərtləndirən mühüm resurs rolunu oynayır. Texnologiyada irəliləyişlər və informasiyaya əlçatanlıq aktivlərin dəyəri ilə bağlı ənənəvi fikirləri gücləndirir. Əgər aqrar cəmiyyətdə torpaq, sənaye cəmiyyətində isə kapital əsas sərvət idisə, müasir informasiya cəmiyyətində informasiya rəqabət qabiliyyətini və inkişafı şərtləndirən əsas resursa çevrilib. İnformasiya sadəcə faktlar toplusu deyil, onun tətbiqi və istifadəsi kontekstində dəyəri vardır. İnformasiya təhlükəsizliyi sahəsində informasiya təhdid və risklərdən qorunmağı tələb edən aktiv kimi baxılır. Bu, vacib məlumatların sızmasının və ya itirilməsinin təkcə təşkilatlara deyil, bütövlükdə cəmiyyətə də ciddi ziyan vura biləcəyi barədə məlumatlılığı əks etdirir. İnformasiyanın əsas aktiv kimi qəbul edilməsi həm də ölkələr və regionlar üçün qlobal təsirlərə malikdir. Qlobal rəqabət mühitində informasiya toplamaq, təhlil etmək və istifadə etmək bacarığı rəqabətqabiliyyətliliyin və iqtisadi inkişafın müəyyənedici amilinə çevrilir. Daha effektiv informasiya idarəetmə sistemlərinə malik olan ölkələr və regionlar iqtisadiyyat və elmdən tutmuş siyasi təsirlərə qədər müxtəlif sahələrdə üstünlüklərə malikdir. Beləliklə, informasiyanın əsas sərvət kimi qəbul edilməsi informasiya cəmiyyətinin müasir tendensiyalarını və çağırışlarını, həyatın müxtəlif sahələrində uğur əldə etmək üçün bizlərə nəhəng imkanlar təqdim edir, eyni zamanda müəyyən risklər də daşıyır.

Qeyd olunan informasiya aktivinin təhlükəsizliyi rəqəmsal ekosistemdə əsas rol oynayır. Hər gün məlumatlarımızın məxfiliyini, bütövlüyünü və

əlçatanlığını poza biləcək müxtəlif təhlükələrlə üzləşirik. Təsəvvür edin ki, e-poçt vasitəsilə şəxsi məktub göndərirsiniz. E-poçtunuz icazəsiz girişdən qorunmursa, mesajınızın məxfiliyi pozula bilər və şəxsi məlumatlarınız cinayətkarların əlinə keçə bilər. Və ya tutaq ki, həssas müştəri məlumatlarını saxlayan bir şirkətdə işləyirsiniz. Bu məlumatlar lazımi şəkildə qorunmazsa, oğurlana və ya zədələnə bilər, nəticədə maliyyə itkisi və müştəri etibarının itirilməsi ilə nəticələnə bilər. Başqa bir misal məlumatın mövcudluğu ilə bağlıdır. Təsəvvür edin ki, siz onlayn bankçılıqdan istifadə edirsiniz və birdən bankın serverlərini hədəf alan kiberhücum səbəbindən hesabınıza daxil ola bilmirsiniz. Bu, sizin və bir çox digər müştərilər üçün ciddi narahatlıq və maliyyə itkisi ilə nəticələnə bilər. Son bir ay ərzində neçə kiberhücum barədə eşitmisiniz? Ötən həftə? Hətta bugün? Hücumların sayı astronomik ölçülərə çatıb. Bir hesabata görə, hər ay yeni zərərli proqram buraxılışlarının sayı 20 milyonu ötür və mövcud zərərli proqramların ümumi sayı 900 milyon nümunəyə yaxınlaşır.

İnformasiyaya icazəsiz giriş, icazəsiz istifadə və hakerlik, piratçılıq və kompüter virusları kimi təhdidlər fərdlər, təşkilatlar və bütövlükdə cəmiyyət üçün ciddi risklər yaradır.

İnformasiya təhlükəsizliyinin əsas problemlərindən biri informasiya sistemlərinin kiberhücumlara qarşı həssaslığıdır. Rəqəmsal təhdidlərin sayının artması və kibercinayətkarlıq texnologiyalarının inkişafı ilə həm maliyyə institutlarına, həm iri korporasiyalara, həm də sıravi istifadəçilərə ciddi ziyan vura biləcək yeni hücum üsulları ortaya çıxır. Qeyd etmək lazımdır ki, bu təhlükələr təkcə texniki aspektlərlə məhdudlaşmır, həm də sosial mühəndislik, fişinq və digər manipulyasiya üsullarını əhatə edir.

İnformasiya təhlükəsizliyi problemlərinin həlli kompleks yanaşma tələb edir. Müasir antivirus proqramlarının, firewallların və müdaxilənin aşkarlanması sistemlərinin istifadəsi kimi təkcə texniki mühafizə tədbirlərini deyil, həm də istifadəçilərin təhlükəsizlik qaydalarına öyrədilməsi və mümkün təhlükələr barədə məlumatlılığının təmin edilməsi vacibdir. Bundan əlavə, təşkilatlar daxilində ciddi informasiya təhlükəsizliyi siyasətinin hazırlanması, monitorinq və audit proseslərinin həyata keçirilməsi, kibercinayətkarlıqla mübarizə üçün digər təşkilatlar və hüquq-mühafizə orqanları ilə əməkdaşlıq etmək lazımdır.

İnformasiya təhlükəsizliyi təkcə texniki məsələ deyil, həm də bütün cəmiyyətdən diqqət və səy tələb edən təhlükəsizlik mədəniyyəti məsələsidir. Texnologiyanın inkişafı və cəmiyyətin şəbəkə resurslarından asılılığının

artması ilə informasiya və məlumatların təhlükəsizliyi ilə bağlı yeni təhdidlər və problemlər yaranır. Bundan əlavə, şəbəkə təhlükəsizliyi problemlərinin aktuallığı rəqəmsallaşmanın həyatın müxtəlif sahələrində, o cümlədən biznes, təhsil, səhiyyə, dövlət xidmətləri və s. tətbiqi ilə daha geniş vüsət almışdır. Şəbəkədə kibertəhlükələrin və kiberhücumların artımı birbaşa məlumatın məxfiliyi, bütövlüyü və əlçatanlığı üçün ciddi risklər yaradır. Bu amilləri nəzərə alaraq, şəbəkə təhlükəsizliyinin təmin edilməsi həm təşkilati səviyyədə, həm də bütövlükdə cəmiyyət səviyyəsində informasiya resurslarının idarə edilməsinin tərkib hissəsinə çevrilir. Onlayn təhdidlərdən qorunmaq və təhlükəsiz rəqəmsal gələcəyi təmin etmək üçün yüksək səviyyədə məlumatlılığın qorunması, qabaqcıl texnologiya həllərinin tətbiqi və ciddi təhlükəsizlik siyasətlərinin işlənib hazırlanması zərurətə çevrilir.

TƏHLÜKƏSİZLİYİN NÖVLƏRİ VƏ STANDARTLARI

Təhlükəsizlik növləri[2] məlumat və sistemlərin mühafizəsinin müxtəlif aspektlərini əhatə edir. Əsas təhlükəsizlik növlərinə aşağıdakılar daxildir:

- İnformasiya təhlükəsizliyi.
- Şəbəkə təhlükəsizliyi.
- Fiziki təhlükəsizlik.
- Tətbiq təhlükəsizliyi.
- Kriptoqrafik təhlükəsizlik.
- Korporativ təhlükəsizlik.
- Kibertəhlükəsizlik.
- Mobil təhlükəsizlik.

İnformasiya Təhlükəsizliyi məlumatın məxfiliyini, bütövlüyünü və əlçatanlığını icazəsiz girişdən, dəyişdirilmədən və ya məhv edilməsindən qorumaq məqsədi daşıyır. İnformasiya təhlükəsizliyinin əsas məqsədi məlumatın məxfiliyini, bütövlüyünü və əlçatanlığını təmin etməkdir. Bu məqsədə nail olmaq üçün məlumatların şifrələnməsi, girişə nəzarət sistemlərinin quraşdırılması, şəbəkə fəaliyyətinin monitorinqi, kadrların informasiya təhlükəsizliyi qaydalarına öyrədilməsi kimi müxtəlif üsullardan istifadə olunur. Bundan əlavə, informasiya təhlükəsizliyi həm müdaxilə

[2] Əliquliyev R. M., İmamverdiyev Y.N. "İnformasiya təhlükəsizliyi insidentləri". Bakı - 2012, 219 s.

edənlərdən (hakerlər, viruslar, kiberhücumlar), həm də işçilərin səhvləri və ya təşkilat daxilində məlumatlara icazəsiz girişdən yaranan daxili təhlükələrdən qorunmağa yönəlib. Beləliklə, informasiya təhlükəsizliyinin əsas məqsədi informasiyanın bütün mümkün təhlükələrdən qorunmasını təmin etmək və onun məxfiliyini, bütövlüyünü və əlçatanlığını qorumaqdır.

İnformasiya təhlükəsizliyinin predmeti təşkilat və ya fərd üçün qiymətli aktiv olan təhlükə və risklərdən qorunma tələb edən bütün verilənləri əhatə edir. Məsələn, verilən və informasiya obyekti timsalında mətn sənədləri, elektron cədvəllər, verilənlər bazası, multimedia faylları, e-poçt və s. daxil olmaqla istənilən məlumat forması ola bilər. İnformasiya sistemləri və şəbəkələri timsalında kompüterlər, serverlər, smartfonlar, marşrutlaşdırıcılar, açarlar və s.

Proqram təminatı timsalında əməliyyat sistemləri, tətbiqi proqram təminatı və informasiya təhlükəsizliyi proqramları (antivirus proqramı, firewall və s.) və tətbiülər nəzərdə tutulur. İnsanlar və proseslər timsalında isə təhlükəsizlik siyasətləri, autentifikasiya və avtorizasiya prosedurları və personal üçün təhlükəsizlik təlimi nəzərdə tutulur. Fiziki Resurslar timsalında fiziki infrastrukturun qorunması, o cümlədən server otaqları, məlumat mərkəzləri, kompüter otaqları və s. nəzərdə tutulur. Əsasən, informasiya təhlükəsizliyi predmetinə informasiyanın emalı, saxlanması və ötürülməsi ilə bağlı bütün proseslər, eləcə də ona təsir edə bilən amillər, məsələn, insanlar, texnologiya, proseslər və ətraf mühit daxildir.

Şəbəkə təhlükəsizliyi – kompüter şəbəkələrinin və onlarla əlaqəli cihazların kiberhücumlardan, o cümlədən zərərli proqramlar, hacklər və şəbəkə hücumlarından qorunması ilə məşğul olan sahədir.

Fiziki təhlükəsizlik – məlumat və ya sistemləri ehtiva edən fiziki avadanlıq və binaları icazəsiz girişdən və ya zədələnmədən qorumaq üçün nəzərdə tutulmuş tədbirləri əhatə edir.

Tətbiq təhlükəsizliyi – proqram təminatı və tətbiqlərin zəifliklərdən, istismarlardan və onların zəif tərəflərini hədəf alan hücumlardan qorunmasını təmin etməklə məşğuldur.

Kriptoqrafik təhlükəsizlik – məlumatları şifrələmək və imzalamaqla qorumaq üçün kriptoqrafik texnika və alqoritmlərdən istifadəni nəzərdə tutur.

Veb tətbiq təhlükəsizliyi – veb saytları və veb proqramları SQL inyeksiyaları, saytlar arası skriptlər və s. kimi müxtəlif təhlükələrdən qorumaqda ixtisaslaşan proqram təhlükəsizliyi bölməsidir.

Korporativ təhlükəsizlik – işçi heyətinin, aktivlərinin və nüfuzunun qorunması da daxil olmaqla bütövlükdə təşkilatın təhlükəsizliyini təmin etməyə yönəlmiş siyasət, prosedur və tədbirlərin hazırlanması və həyata keçirilməsi ilə əlaqədardır.

Kibertəhlükəsizlik – məlumatın məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək, həmçinin informasiya sistemlərini və şəbəkələrini icazəsiz girişdən, məlumat sızmasından və digər növ kiberhücumlardan qorumaqdır. Bu məqsədə nail olmaq üçün kibertəhlükəsizlik mütəxəssisləri məlumatların şifrələnməsi, firewall, antivirus proqramı, müdaxilənin aşkarlanması sistemləri, autentifikasiya və avtorizasiya, şəbəkə fəaliyyətinin monitorinqi və s. kimi müxtəlif üsul və texnologiyalardan istifadə edirlər.

Mobil təhlükəsizlik – mobil cihazların, proqramların və məlumatların istifadəsi ilə bağlı müxtəlif təhlükələrdən qorunmasına yönəlmiş tədbirləri əhatə edir.

Bu təhlükəsizlik növlərinin hər biri öz xüsusiyyətlərinə malikdir və informasiya və sistemlərin effektiv mühafizəsini təmin etmək üçün xüsusi tədbirlər tələb edir.

Təhlükəsizlik standartları[3]. İnformasiya təhlükəsizliyi mərkəzləşdirilmiş şəkildə inzibati, texniki və fiziki aspektlərin təhlükəsizliyini[4] təmin edən kompleks bir prosesdir. Qeyd olunan aspektlərdə təhlükəsizliyin təmin olunması ilə bağlı istifadə olunan standartları aşağıdakı kimi qruplaşdırmaq olar:

1. İnzibati təhlükəsizliyi təmin edən standartlar.
2. Fiziki təhlükəsizliyi təmin edən standartlar.
3. Texniki təhlükəsizliyi təmin edən standartlar.

Hər 3 istiqamətdə istifadə olunan standartları aşağıdakı kimi qruplaşdırımaq olar: ISO/IEC 27001, CISA və CISSP. İnzibati təhlükəsizliyi təmin edən standartların domenləri cədvəl 1.1-də təsvir olunmuşdur.

[3] Rzayeva G., İbrahimova A. Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi. Dərs vəsaiti. Bakı: "Nurlar" nəşriyyatı, 2021, 200 s.
Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.

[4]

Cədvəl 1.1

İnzibati təhlükəsizliyi təmin edən standartların domenləri

İstiqamət	ISO/IEC 27001	CISA	CISSP
İNZİBATİ	İnformasiya təhlükəsizliyi siyasəti	İT üzrə nəzarət və idarəetmə	Təhlükəsizlik sisteminin infrastukturu və texnikası
	İnformasiya təhlükəsizliyi təşkilatı	-	-
	Aktivlərin idarə olunması	İnformasiya aktivlərinin qorunmas	-
	İnsan resurslarının təhlükəsizliyi	-	-
	İnformasiya təhlükəsizliyi ilə bağlı hadisələrə nəzarət	-	-
	İşin davamlılığının informasiya təhlükəsizliyi aspektləri	-	-
	Təchizatçı ilə əlaqələr Uyğunluq	İnformasiya sistemləri (İS) üzrə audit prosesi	Təhlükəsizliyin qiymətləndirilməsi və sınaqdan keçirmə

İnzibati standartlar informasiya təhlükəsizliyinin idarə edilməsi proseslərini, o cümlədən siyasətlərin, prosedurların və təlimatların işlənib hazırlanmasını və təhlükəsizliyin effektiv idarə edilməsini təmin etmək üçün təşkilati strukturu müəyyən edir. Fiziki təhlükəsizliyi təmin edən standartların domenləri cədvəl 1.2-də təsvir olunmuşdur.

Cədvəl 1.2

Fiziki təhlükəsizliyi təmin edən standartların domenləri

İstiqamət	ISO/IEC 27001	CISA	CISSP
FİZİKİ	Fiziki və mühit təhlükəsizliyi		Aktivlərin təhlükəsizliyi

Fiziki standartlar girişə nəzarət rejimləri, videomüşahidə, girişə nəzarət sistemləri və s. istifadə etməklə məlumat mərkəzləri, server otaqları və digər fiziki obyektlərin təhlükəsizliyini təmin etmək üçün tövsiyələr verir. Texniki təhlükəsizliyi təmin edən standartların domenləri cədvəl 1.3-də təsvir olunmuşdur.

Cədvəl 1.3

Texniki təhlükəsizliyi təmin edən standartların domenləri

İstiqamət	ISO/IEC 27001	CISA	CISSP
TEXNİKİ	Kriptoqrafiya Kommunikasiyanın təhlükəsizliyi Əməliyyatların təhlükəsizliyi		Təhlükəsizliklə bağlı əməliyyatlar Kommunikasiya və şəbəkə təhlükəsizliyi
	Daxil olmaya nəzarət		Şəxsiyyətin təsdiqi və girişin idarə idərə edilməsi
	Sistemlərin əldə olunması, inkişaf etdirilməsi və onlara xidmət	İnformasiya sistemlərinin əldə olunması, inkişaf etdirilməsi və tətbiqi	Proqram təminatının hazırlanması Təhlükəsizlik

Texniki standartlar texnologiya və təhlükəsizlik tədbirlərinə tələbləri müəyyən edir, məsələn məlumatların şifrələnməsi, autentifikasiya mexanizmləri, zərərli proqramlardan qorunma və şəbəkələrdə, proqramlarda və sistemlərdə məlumatı mühafizəsi və s.

Cədvəl 1.1-1.3-də göstərilən standartlar təşkilatlara riskləri effektiv şəkildə idarə etməyə və informasiyanı kiberhücumlar, məlumat sızması, təhlükəsizlik pozuntuları və digər insidentlər də daxil olmaqla müxtəlif təhlükə və risklərdən qorumağa kömək edən bir sıra təlimatlar, prosedurlar və

təcrübələr təqdim edir. Bu standartların istifadəsi təşkilatın müxtəlif sahələrində əlaqələndirilmiş şəkildə fəaliyyət göstərən, informasiyanın potensial təhlükə və risklərdən tam mühafizəsini təmin edən təhlükəsizlik sistemi yaratmağa imkan verir. Bu, təşkilatın təhlükəsizlik insidentlərinə qarşı dayanıqlığını yaxşılaşdırmağa, müştərilərin və tərəfdaşların etibarını artırmağa, qanuni və normativ tələblərə əməl etməyə və biznes proseslərinin düzgün işləməsini təmin etməyə kömək edir. Buna görə də, təhlükəsizlik standartlarından istifadə müasir rəqəmsal dünyada etibarlı və təhlükəsiz informasiya mühitinin yaradılması üçün əsas elementdir.

TƏHLÜKƏSİZLİK ANLAYIŞLARI VƏ TERMİNLƏRİ

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AZƏRBAYCAN RESPUBLİKASININ QANUNU[5], I fəsil, Maddə 2. Qanunda aşağıdakı anlayışlar işlədilmişdir:

İnformasiya –yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar.

Sənədləşdirilmiş informasiya (sənəd) – maddi daşıyıcıda mətn, səs və ya təsvir formasında qeydə alınan və identikləşdirməyə imkan verən istənilən rekvizitli informasiya mənbəyindən, saxlanma yerindən, rəsmi statusundan, mülkiyyət növündən, mənsub olduğu təşkilat tərəfindən yaradılıb-yaradılmadığından asılı olmayaraq sənədləşdirilmiş informasiya.

Açıq informasiya – əldə olunması, işlənməsi, verilməsi və ya istifadəsi Azərbaycan Respublikasının qanunvericiliyi ilə məhdudlaşdırılmayan və ümumi istifadə üçün təyin olunmuş sənədləşdirilmiş informasiya.

Konfidensial informasiya – vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə olunmasına məhdudiyyət qoyulan məlumatlar, habelə peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri.

[5] Azərbaycan Respublikası Prezidentinin "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə" 1998-ci il 19 iyun tarixli 729 nömrəli Fərmanı.https://mincom.gov.az/storage/pages/1127/ac4cd5b4ed930c3a249aec39e8c71e01.pdf

İnformasiya prosesləri – informasiyanın yaradılması, yığılması, işlənməsi, saxlanması, axtarışı, yayılması.

İnformasiya texnologiyaları – informasiya prosesləri zamanı, o cümlədən hesablama və rabitə texnikasının tətbiqi ilə istifadə edilən üsul və vasitələr sistemi.

İnformasiya sistemi – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklə, nizamlanmış məcmusu.

İnformasiya ehtiyatları – informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda, məlumat banklarında və s.) olan sənədlər və sənəd massivləri, habelə ayrıca mövcud olan sənədlər və onların massivləri.

İnternet informasiya ehtiyatı – internet şəbəkəsində yaradılan, informasiyanın yayılması üçün istifadə olunan, müraciət edilməsi üçün domen adına və sahibi tərəfindən müəyyənləşdirilmiş digər işarələnməyə malik olan informasiya ehtiyatı.

İnternet informasiya ehtiyatının sahibi – internet informasiya ehtiyatından istifadə edilməsi, o cümlədən burada informasiya yerləşdirilməsi qaydalarını sərbəst olaraq müəyyən edən, internet informasiya ehtiyatına sahiblik və istifadə hüquqlarına malik olan şəxs.

Domen adı - internet şəbəkəsində yerləşdirilən informasiya ehtiyatına müraciətin təmin olunması üçün verilən unikal simvol düzülüşü;

Domen adının sahibi - müqaviləyə əsasən domen adına müddətli sahiblik edən şəxs.

İnternet provayder – internet şəbəkəsinə telekommunikasiya vasitələri ilə qoşulmaq üçün texniki imkanı təmin edən təchizatçı;

Host provayder – internet informasiya ehtiyatının istifadəsinin təmin edilməsi üçün öz informasiya sistemlərində yerləşdirilməsi xidmətini göstərən təchizatçı.

Domen adlarının milli inzibatçısı – “az” ölkə kodlu yüksək səviyyəli domen zonasında domen adlarının inzibatçılığını həyata keçirən səlahiyyətli şəxs.

Domen adlarının qeydiyyatçısı – domen adların milli inzibatçısı ilə bağlanılmış müqaviləyə əsasən “az” ölkə kodlu yüksək səviyyəli domen zonasında domenlərin qeydiyyatı üzrə xidmət göstərən şəxs.

İnformasiya sistemləri və texnologiyalarının təminat vasitələri – informasiya sistemlərinin və texnologiyalarının yaradılması zamanı hazırlanan və onların istismarını təmin edən proqram, texniki, linqvistik, hüquqi, təşkilati vasitələr.

İnformasiya sistemləri, texnologiyaları, ehtiyatları və onların təminat vasitələrinin mülkiyyətçisi – göstərilən obyektlər üzərində tam sahiblik, istifadə, sərəncamvermə hüququnu həyata keçirən subyekt.

İnformasiya sistemləri texnologiyaları, ehtiyatları və onların təminat vasitələrinin sahibi – göstərilən obyektlər üzərində qanunla müəyyən olunmuş qaydada sahiblik və istifadə hüququnu həyata keçirən subyekt.

İnformasiyanın istifadəçisi – özü üçün zəruri informasiyanın alınması məqsədilə bilavasitə informasiya sisteminə və ya vasitəçiyə müraciət edən və ondan ancaq istifadə hüququna malik subyekt.

İnformasiya məhsulları – istifadəçilərin tələblərinə əsasən yaradılmış və onların tələbatlarının ödənilməsi üçün təyin olunmuş və ya tətbiq edilən sənədləşdirilmiş informasiya, informasiya sistemləri, texnologiyaları və onların təminat vasitələri;

İnformasiya xidmətləri – istifadəçilərin informasiya məhsulları ilə təmin edilməsi üzrə subyektlərin (mülkiyyətçilər, sahiblər və ya vasitəçilərin) fəaliyyəti;

İnformasiyalaşdırma – informasiya ehtiyatlarının formalaşdırılması, təqdim edilməsi, istifadə olunması əsasında dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların informasiya tələbatlarının və bu sahədəki hüquqlarının təmin edilməsinin optimal şəraitinin yaradılması üçün təşkilati, sosial-iqtisadi və elmi-texniki proses;

Kritik informasiya infrastrukturu – dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ya ekologiya sahəsində fəaliyyəti təmin edən və funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vura bilən informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin məcmusu;

Kritik informasiya infrastrukturu obyekti – kritik informasiya infrastrukturunun tərkib hissəsi olan informasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və ya informasiya-kommunikasiya şəbəkəsi;

Kritik informasiya infrastrukturu subyekti – kritik informasiya infrastrukturu obyektinin sahibi (istifadəçisi) olan dövlət orqanları (qurumları), o cümlədən dövlətə məxsus olan hüquqi şəxslər, dövlət adından

yaradılmış publik hüquqi şəxslər, habelə digər hüquqi şəxslər və ya fərdi sahibkarlar (mikro, kiçik və orta sahibkarlıq subyektləri istisna olmaqla);

Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində səlahiyyətli orqan (bundan sonra - səlahiyyətli orqan) – kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi məqsədilə bu qanunla və bu qanundan irəli gələn digər normativ hüquqi aktlarla müəyyən edilmiş funksiyaları yerinə yetirən müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum);

Kibertəhlükəsizlik xidməti provayderi – kibertəhlükəsizlik xidmətlərinin göstərilməsi sahəsində fəaliyyət göstərən, işçi heyəti, texnoloji resursları və proseslərinə dair müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilən tələblərə cavab verən və kritik informasiya infrastrukturu subyekti ilə bağlanılmış müqavilə əsasında onlara kibertəhlükəsizlik xidməti göstərən hüquqi şəxslər;

İnformasiya təhlükəsizliyi – informasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsi;

Kibertəhdid – informasiya sistemlərinə və ya ehtiyatlarına qanunsuz daxilolma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına səbəb ola bilən amil və ya vəziyyət;

Kiberhücum – informasiya sistemlərinin və ya ehtiyatlarının informasiya təhlükəsizliyinə təhdid yaradan, yaxud onların fəaliyyətinin pozulmasına və ya dayanmasına səbəb olan kiberməkan vasitəsilə qəsdən törədilən əməl;

Kiberinsident – informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin fəaliyyətinin dayanması və ya pozulması, yaxud həmin obyektlərdə informasiya təhlükəsizliyinin pozulmasına səbəb olan hadisə.

Bununla yanaşı əsas təhlükəsizlik proseslərini və konsepsiyalarını başa düşmək məlumat və sistemləri effektiv şəkildə qorumaq üçün əsasən aşağıdakı terminlərin öyrənilməsi məqsədəuyğundur[6].

Təhdid – Məlumata və ya sistemə zərər verə biləcək potensial təhlükəsizlik pozuntusu.

[6] İsmayıl Calallı (Sadıqov), "İnformatika terminlərinin izahlı lüğəti", 2017, "Bakı" nəşriyyatı, 996 s.

Zəiflik – Təhlükəsizliyi pozmaq üçün təcavüzkar tərəfindən istifadə edilə bilən sistemdəki zəif nöqtə.

Risk – Təhlükənin və ya zəifliyin istismar olunma ehtimalı və belə hadisələrin mümkün nəticələri.

Mühafizə – Təhdidlərin qarşısını almaq və ya azaltmaq və məlumat və sistemlər üçün riskləri azaltmaq üçün görülən tədbirlər və texnologiyalar.

Autentifikasiya – Etibarnamələri təqdim edən subyektin (istifadəçi, cihaz və ya sistem) şəxsiyyətinin yoxlanılması prosesi.

Avtorizasiya – Uğurlu autentifikasiyadan sonra müəyyən resurslara və ya funksiyalara giriş hüquqlarının verilməsi prosesi.

Şifrələmə – Xüsusi alqoritm və açardan istifadə etməklə məlumatın kənar şəxslər üçün anlaşılmaz formaya çevrilməsi prosesi.

Multi-faktor Authentication (MFA) – İstifadəçinin şəxsiyyətini yoxlamaq üçün iki və ya daha çox amildən istifadə edən autentifikasiya üsulu, məsələn, parol və mobil telefonda qəbul edilən kod.

Biometrik Doğrulama – Barmaq izləri, üz tanıma və ya səsin tanınması kimi şəxsin bioloji xüsusiyyətlərinə əsaslanan autentifikasiya üsulu.

Fişinq – Təcavüzkarların məxfi məlumat əldə etmək üçün özlərini etibarlı şəxslər və ya təşkilatlar kimi təqdim edərək istifadəçiləri aldatmağa çalışdıqları bir fırıldaq növü.

Firewall – Şəbəkəni icazəsiz giriş və hücumlardan qorumaq üçün müəyyən edilmiş təhlükəsizlik qaydaları əsasında şəbəkə trafikini izləyən və filtrləyən şəbəkə cihazı və ya proqram təminatı.

Zərərli proqram – İstifadəçinin kompüterinə, şəbəkəsinə və ya məlumatlarına zərər vermək üçün nəzərdə tutulmuş viruslar, qurdlar, troyan atları, casus proqramlar və reklam proqramları kimi zərərli proqramların ümumi adı.

Xidmətdən imtina (DoS) – Təcavüzkarın hədəf sistemi və ya şəbəkəni həddən artıq yükləməyə və ya əlçatmaz hala gətirməyə cəhd etdiyi və ona hüquqi girişin qarşısını aldığı kiberhücum növü.

Perimetr Təhlükəsizliyi – İcazəsiz girişin qarşısını almaq və daxili resursları qorumaq üçün şəbəkə və ya sistemin xarici sərhədlərində tətbiq edilən təhlükəsizlik tədbirləri.

Təhlükəsizlik Siyasəti – Təşkilatda məlumat və sistemlərin təhlükəsizliyini təmin etmək üçün qaydaları, prosedurları və təlimatları təsvir edən sənəd.

Yedəkləmə – Əsas verilənlər itirildikdə, zədələndikdə və ya məhv edildikdə bərpasını təmin etmək üçün məlumatların surətlərinin yaradılması və saxlanması prosesi.

Təhlükəsizlik Yeniləmələri – Boşluqları aradan qaldırmaq və sistemin təhlükəsizliyini təmin etmək üçün hazırlanmış yamaqlar, düzəlişlər və proqram yeniləmələri.

Rəqəmsal İmza – Məzmuna unikal elektron imza əlavə etməklə elektron sənədin və ya mesajın həqiqiliyini və bütövlüyünü yoxlamağa imkan verən mexanizm.

Bulud Təhlükəsizliyi – Bulud mühitində saxlanılan və emal edilən məlumatları, tətbiqləri və infrastrukturu qorumaq üçün istifadə edilən təhlükəsizlik tədbirləri.

Etik Haker – Sistemi və ya şəbəkəni həqiqi hakerlərə qarşı sınaqdan keçirmək və sərtləşdirmək üçün hakerlik və hücum üsullarından istifadə edən informasiya təhlükəsizliyi üzrə mütəxəssis.

İdentifikasiya – Şəxsiyyəti təqdim edən istifadəçi, cihaz və ya proqram kimi obyektin müəyyən edilməsi prosesi.

Şəbəkə Təhdidləri – Trafikin ələ keçirilməsi, xidmətlərə hücumlar və zəifliklərin istismarı daxil olmaqla kompüter şəbəkələrini hədəf alan təhlükələr.

Sosial Mühəndislik – Təcavüzkarlar tərəfindən istifadəçiləri aldatmaq və məxfi məlumat əldə etmək üçün istifadə olunan manipulyasiya üsulları.

Patch – Zəiflikləri və ya təhlükəsizlik xətalarını düzəltmək üçün tərtibatçı tərəfindən buraxılmış proqram yeniləməsi.

Kriptoqrafiya – Məlumatların başqalarının başa düşə bilməyəcəyi formaya çevrilməsi yolu ilə məxfiliyini, bütövlüyünü və autentifikasiyasını təmin etmək üsulları haqqında elmdir.

İnsayder – Daxili istifadəçilər və ya təşkilatın işçiləri tərəfindən yaranan təhlükələrin qarşısını almaq və aşkar etmək üçün nəzərdə tutulmuş təhlükəsizlik tədbirləri.

Təhlükəsizlik sertifikatlaşdırması – Sistemin, məhsulun və ya xidmətin təhlükəsizlik standartlarına və tələblərinə cavab verdiyini qiymətləndirmək və yoxlamaq prosesi.

Təhlükəsizlik protokolu – Sistem iştirakçıları arasında təhlükəsiz məlumat mübadiləsini müəyyən edən qaydalar və prosedurlar toplusu.

Təhdidlərin idarə edilməsi – İnformasiya və sistemlərin təhlükəsizliyini təmin etmək üçün təhdidlərin müəyyən edilməsi, qiymətləndirilməsi, monitorinqi və idarə edilməsi prosesi və üsulları.

Təhlükəsizlik əməliyyatları mərkəzi (SOC) – Təhlükəsizlik hadisələrinin müəyyən edilməsi, təhlili və cavablandırılması üçün cavabdeh olan mərkəzləşdirilmiş təhlükəsizlik idarəetməsi və monitorinq nöqtəsi.

Xidmətdən imtina (DoS) – Hədəf sisteminin və ya şəbəkənin resurslarını qanuni istifadəçilər üçün əlçatmaz etmək üçün həddən artıq yükləmək üçün nəzərdə tutulmuş kiberhücum.

Paylanmış xidmətdən imtina (DDoS) – Təcavüzkarların hədəf sistemə və ya şəbəkəyə eyni vaxtda hücum etmək üçün bir neçə kompüter və ya cihazdan istifadə etdiyi kiberhücum növü.

Girişin İdarə Edilməsi – Bu hüquqların təyin edilməsi, dəyişdirilməsi və ləğvi daxil olmaqla, istifadəçilərin və ya cihazların informasiya sistemi resurslarına giriş hüquqlarının idarə edilməsi prosesi.

Təhlükəsizlik İnsidenti – Məlumatın, sistemin və ya şəbəkənin təhlükəsizliyinə təhlükə yaradan gözlənilməz hadisə və dərhal reaksiya tələb olunur.

Hücumun aşkarlanması və qarşısının alınması – kompüter sisteminə və ya şəbəkəyə icazəsiz müdaxilələrin aşkarlanması və bloklanması texnologiyaları və üsulları.

Mərkəzləşdirilmiş giriş – Anomaliyaları və təhlükəsizlik insidentlərini aşkar etmək üçün müxtəlif mənbələrdən qeydlərin və hadisələrin toplanması və təhlili prosesi və təcrübəsi.

IoT təhlükəsizliyi (Əşyaların İnterneti Təhlükəsizliyi) – Əşyaların İnternetinə daxil olan cihazları və şəbəkələri kiberhücumlardan və təhdidlərdən mühafizə etməyə yönəlmiş tədbirlər və texnologiyalar.

Parol siyasəti – İstifadəçi parollarının yaradılması, saxlanması və istifadəsi üçün onların təhlükəsizliyini təmin etməyə yönəlmiş qaydalar və tələblər toplusu.

Rəqəmsal təhlükəsizlik – Rəqəmsal mühitdə informasiyanın, sistemlərin və cihazların müxtəlif təhlükə və risklərdən qorunmasını təsvir edən ümumi termindir.

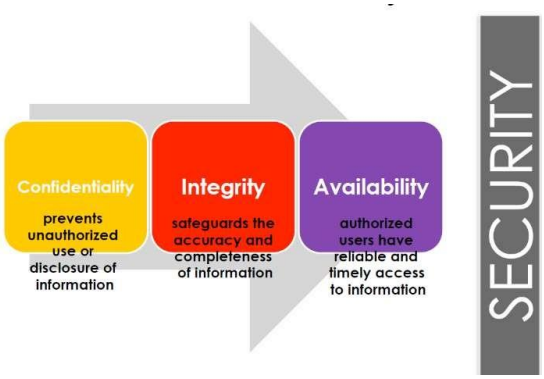
İstifadəçi təlimi – Bir təşkilatın işçilərinə və ya istifadəçilərinə rəqəmsal mühitdə informasiya təhlükəsizliyinin əsasları və düzgün davranış öyrədilməsi prosesi.

Bu terminlər və anlayışlar təhlükəsizlik prinsiplərini başa düşmək üçün əsasdır və rəqəmsal dünyada təhdid və risklərə effektiv cavab verməyə kömək edir.

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ÜÇLÜ MODELİ

İnformasiya təhlükəsizliyi heç vaxt uğurlu hücumların qarşısını tam ala bilməz və ya tam sistem təhlükəsizliyinə zəmanət verə bilməz, necə ki, ev üçün görülən təhlükəsizlik tədbirləri heç vaxt oğrudan tam təhlükəsizliyə zəmanət verə bilməz.

İnformasiya təhlükəsizliyinin əsas məqsədi[7] hücumları dəf etmək üçün qoruyucu tədbirlərin düzgün tətbiq edilməsini təmin etmək, uğurlu hücum zamanı sistemin fəaliyyətinin tam pozulmasının qarşısını almaq və mümkün qədər tez bərpa etməkdir. Beləliklə, informasiya təhlükəsizliyi birincisi müdafiə mexanizmidir, ikincisi, istifadəçilər və biznes proseslər üçün dəyərli olan məlumatları qorumaq üçün nəzərdə tutulmuşdur (şəkil 1.2).



Şəkil 1.2. CIA QANUNU

CIA Triada modeli kimi tanınan məlumat üç qorunmaya məruz qalmalıdır:

[7] Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011, 112 s.
Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации: учеб. пособие / Н.В. Келдыш. - М.: Мир науки, 2022. – сетевое издание. Режим доступа: https://izdmn.com/PDF/14ЬТТ3Г22.pdf
https://www.javatpoint.com/cyber-security-tutorial

1. Məxfilik. İnformasiyanın məzmunundan irəli gələrək, ona müraciət etmə ilə bağlı məhdudiyyətləri nəzərdə tutur. Məxfilik proqram təminatından tutmuş veb serverlərdə saxlanılan fərdi məlumatların (məsələn, kredit kartı, tibbi, hərbi, təhsil məlumatları və s.) şifrələnməsi və həmin serverlərə icazəsiz girişin qarşısını almaq üçün müdafiə mexanizmlərini icra edən təhlükəsizlik alətlərini əhatə edir.

2. Tamlıq. İnformasiyanın təhrifsiz şəkildə mövcud olmasını nəzərdə tutur. Məsələn, onlayn alış-veriş nümunəsində, alış məbləğini 10.000 dollardan 1 dollara dəyişə bilən pis niyyətli hakerlər məlumatın bütövlüyünü pozacaq.

3. Əlçatanlıq. İstənilən zaman lazımi informasiyanın əldə edilə bilmə imkanı, eləcə də müxtəlif informasiyanın əldə edilməsinə yönəlmiş müraciətin cavablandırılması üçün uyğun xidmətlərin həmişə hazır olması deməkdir. Məsələn, onlayn alışdan sifariş edilən məhsulların ümumi miqdarı anbar əməkdaşına açıq olmalıdır ki, nəzərdə tutulan mallar müştəriyə göndərilə bilsin, lakin bu məlumatlar kiber dələduzlar üçün əlçatan olmamalıdır.

İnformasiya kompüter avadanlığında saxlandığı, proqram təminatı ilə işləndiyi və kommunikasiyalar vasitəsilə ötürüldüyü üçün bu sahələrin hər biri qorunmalıdır.

Beləliklə, informasiya təhlükəsizliyinin üçlü modeli üç əsas komponenti özündə birləşdirən informasiya təhlükəsizliyinə konseptual yanaşmadır: məxfilik, bütövlük və əlçatanlıq (CIA). Bu üç aspekt informasiya təhlükəsizliyinin əsas məqsədləridir və informasiya təhlükəsizliyi strategiyalarını, siyasətlərini və mexanizmlərini hazırlamaq üçün istifadə olunur.

TƏHLÜKƏSİZLİK PRİNSİPLƏRİ

Təhlükəsizlik prinsipləri[8] istər informasiya təhlükəsizliyi, istər fiziki təhlükəsizlik, istərsə də iş yerində davranış qaydalarının təhlükəsizliyi olsun, istənilən sahədə təhlükəsizliyi təmin edən fundamental yanaşma və metodologiyalardır. Bu prinsiplər strategiyaların, siyasətlərin və prosedurların hazırlanması üçün əsas baza mexanizmini təşkil edir və istifadəçiləri, aktivləri

[8] Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.

və məlumatları müxtəlif təhlükə və risklərdən qorumaq məqsədi daşıyır. Təhlükəsizlik prinsipləri aşağıdakı aspektləri əhatə edir:

Məxfilik – məlumatın gizli saxlanmasına və ona girişin yalnız səlahiyyətli şəxslərlə məhdudlaşdırılmasına zəmanət verir.

Tamlıq – informasiyanın 2 subyekt (kompüter, şəbəkə avadanlıqları və s.) arasında dəyişdirilmədən ötürülməsini xarakterizə edir.

Əlçatanlıq – məlumatın səlahiyyətli istifadəçilər tərəfindən lazımi vaxtda və yerdə istifadəsi üçün mövcud olmasını təmin edir.

Məlumdur ki, bu 3 prinsip CIA modelini formalaşdırır və bir başa informasiya təhlükəsizliyinin məqsədini əhatə edir.

Autentifikasiya – fiziki şəxsin və ya qurumun şəxsiyyətinin təsdiqlənməsidir.

Avtorizasiya – resurslara və ya məlumatlara girişin yalnız səlahiyyətli istifadəçilər üçün məhdudlaşdırılmış prosesidir.

Bölünməzlik – təhlükəsizliyin ayrı-ayrı hissələrə bölünməməsi və parçalanmaması üçün birliyini qorumaqdır.

Davamlılıq – sistemin və ya təşkilatın həyat dövrü ərzində təhlükəsizliyin davamlılığını və ardıcıllığını təmin etməkdir.

Qarşılıqlı asılılıq – təhlükəsizliyin müxtəlif aspektlərinin necə əlaqəli olduğunu və bir-birinə necə təsir etdiyini başa düşmək və qeydiyyata almaqdır.

Proaktivlik – təhdidlərin qarşısını almaq və riskləri minimuma endirmək üçün ehtiyat və qabaqlayıcı tədbirlər görməkdir.

Təlim və maarifləndirmə – təhdidlərin başa düşülməsini və onların qarşısının alınmasını təkmilləşdirmək üçün heyətin təlimi və təhlükəsizliklə bağlı maarifləndirmə dəstəyini verməkdir.

Bu prinsiplər öz növbəsində aktivlərin və məlumatların qorunması üçün istifadə olunan xüsusi tədbirləri və texnologiyaları müəyyən edən təhlükəsizlik strategiyaları və siyasətlərinin işlənib hazırlanması üçün əsas rol oynayır.

YOXLAMA SUALLARI

1. Təhlükəsizlik nədir və təşkilatlar üçün nə üçün vacibdir?
2. İnformasiya təhlükəsizliyinə təsir edə biləcək əsas təhlükələr hansılardır?
3. Təhlükəsizliyin əsasında hansı prinsiplər dayanır?

4. Təhlükəsizliyin əsas növləri hansılardır?
5. Təhlükəsizlik standartları hansı istiqamətlərdə formalaşdırılır?
6. İnzibati təhlükəsizliyi təmin edən standartlar hansılardır?
7. Fiziki təhlükəsizliyi təmin edən standartlar hansılardır?
8. Texniki təhlükəsizliyi təmin edən standartlar hansılardır?
9. Fiziki, informasiya və kibertəhlükəsizlik hansı aspektləri əhatə edir?
10. Hər bir təhlükəsizlik növü üçün hansı xüsusi təhdidlər xarakterik ola bilər?
11. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik anlayışlarının məqsədi və predmeti geniş təhlil olunmuşdur. Təhlükəsizliyin digər növlərini də bu qaydada təhlil edin.
12. "Təhlükəsizlik siyasəti" termini nəyi nəzərdə tutur?
13. İnformasiya təhlükəsizliyini təmin etmək üçün hansı şərtlər yerinə yetirilməlidir?
14. İnformasiya təhlükəsizliyinin üçlü CIA modeli nədir və hansı komponentlər daxildir?

PRAKTİKİ TAPŞIRIQ

1. Şəxsi hücum təcrübəsi

Siz (dostunuz və ya başqa tələbə) hansı növ kompüter hücumu ilə üzləşmisiniz? Nə vaxt oldu? Hansı növ kompüter və ya cihaz iştirak edirdi? Hansı ziyana səbəb oldu? Hücumdan sonra asayişi bərpa etmək üçün nə edilməlidir? Hücumdan sonra kompüter necə təmir edildi? Bunun qarşısını nə ala bilərdi? Hücumun uğurlu olduğuna inandığınız səbəbi və ya səbəbləri sadalayın. Bu təcrübə haqqında bir səhifəlik sənəd yazın.

2. Təşkilatın təhlükəsizliyinin təhlili

Bir təşkilat seçin (iş yeriniz, təhsil müəssisəniz və ya hər hansı digər struktur ola bilər). Fiziki, informasiya və kibertəhlükəsizlik də daxil olmaqla, cari təhlükəsizlik tədbirlərini qiymətləndirin. Təşkilatınızın təhlükəsizliyinə təsir edə biləcək potensial təhdidləri və zəiflikləri müəyyən edin. Yeni siyasət və texnologiyaların tətbiqi də daxil olmaqla, təşkilatın təhlükəsizliyini yaxşılaşdırmaq üçün fəaliyyət planı hazırlayın.

3. Təhlükəsizlik siyasətinin yaradılması.

Müxtəlif təşkilatların təhlükəsizlik siyasətlərinə dair nümunələri öyrənin və ya ISO 27001 kimi təhlükəsizlik standartlarının təlimatlarından istifadə edin. Tələblərini, təhdidlərini və müdafiəsini nəzərə alaraq, təşkilat üçün təhlükəsizlik siyasətini formalaşdırın.

4. İnformasiya təhlükəsizliyinə dair məlumatlılıq səviyyəsinin qiymətləndirilməsi

Ətrafınızda və ya təşkilatınızda insanlar arasında informasiya təhlükəsizliyinə dair məlumatlılıq səviyyəsini dəyərləndirin.

MODUL 2. ŞƏBƏKƏ CİHAZLARI VƏ TEXNOLOGİYALARI

AKTİV VƏ PASSİV ŞƏBƏKƏ CİHAZLARI
OSI VƏ TCP/ IP MODELİ
PORT NÖMRƏLƏRİ VƏ ŞƏBƏKƏ PROTOKOLLARI
İNTERNET SƏVİYYƏSİNİN PROTOKOLLARI: IPv4 və IPv6
ŞƏBƏKƏ PROBLEMLƏRİNİN ARADAN QALDIRILMASI
VİRTUALLAŞDIRMA TEXNOLOGİYALARI

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

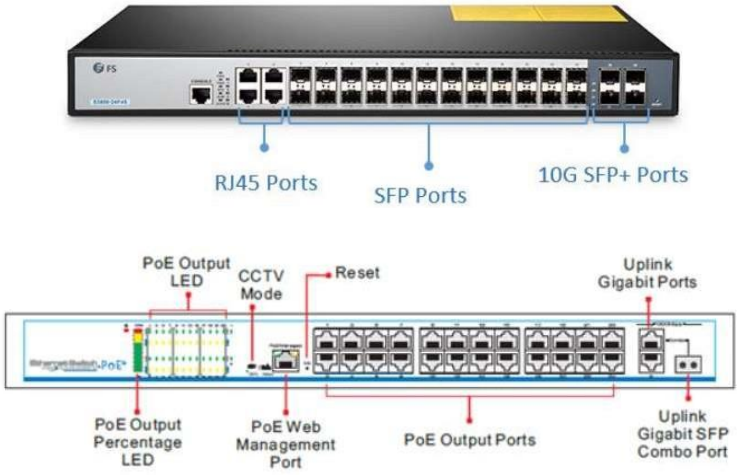
AKTİV VƏ PASSİV ŞƏBƏKƏ CİHAZLARI

Şəbəkə cihazları[9] - kompüter şəbəkəsini təşkil edən qurğulardır. Aktiv və passiv olmaqla iki növ şəbəkə cihazları mövcuddur.

Aktiv şəbəkə cihazları şəbəkə üzərindən ötürülən məlumatları emal etmək və ya çevirmək qabiliyyətinə malik avadanlıqdır. Aktiv şəbəkə cihazlarına aşağıdakılar aiddir:

- **KOMMUTATOR -ŞƏBƏKƏ AÇARI (NETWORKING SWITCH).**
- **MEDİA ÇEVİRİCİSİ (MEDIA CONVERTER).**
- **SFP ÖTÜRÜCÜSÜ / MODUL (SFP TRANSCEIVER / MODULE).**
- **MARŞRUTİZATOR (ROUTERS).**
- **GİRİŞ NÖQTƏLƏRİ (ACCESS POINTS).**
- **POE İNJEKTORLARI (POE INJECTORS).**
- **SERVER PRİNTERLƏRİ (PRINT SERVER).**

KOMMUTATOR - ŞƏBƏKƏ AÇARI (NETWORKING SWITCH). KOMMUTATOR – şəbəkədəki ayrı-ayrı cihazları (şəbəkə seqmentləri) birləşdirən aktiv şəbəkə elementlərindən biridir (şəkil 2.1.).

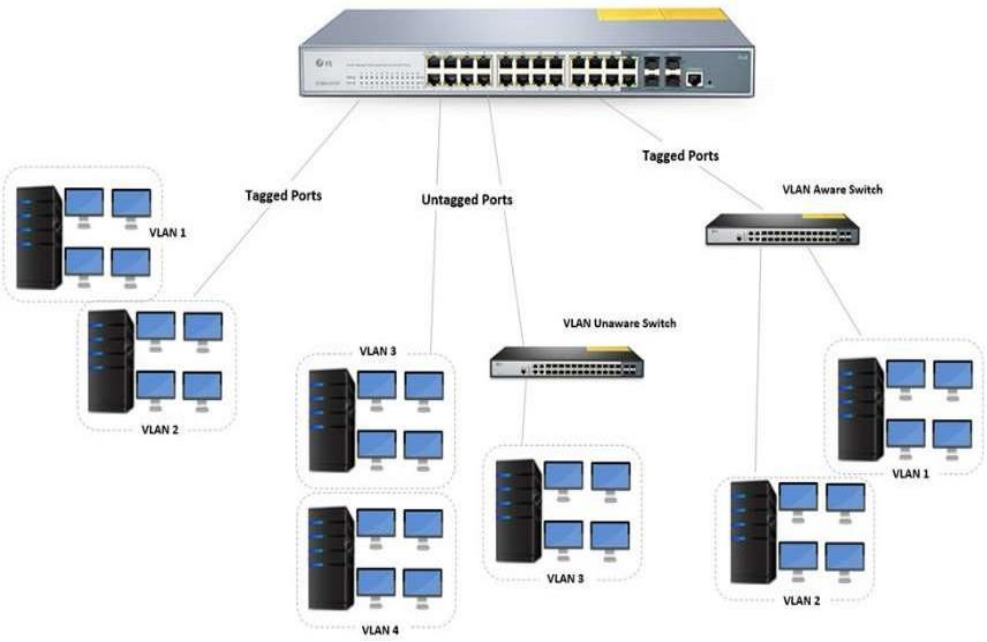


Şəkil 2.1. KOMMUTATOR (NETWORKING SWITCH)

[9] Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.
Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. Издательство Политехнического университета, Санкт-Петербург, 2005.
Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В. 2001, 352 с.

SWITCH lokal şəbəkədə (LAN) kompüterlər, printerlər, serverlər və digər cihazlar arasında əlaqəni təmin edir. Bu qurğu OSI (Open Systems Interconnection) modelinin kanal (Data Link) səviyyəsində işləyir və məlumatları ötürmək üçün MAC ünvanlarından istifadə edirlər. Bu qurğular şəbəkə trafikinin təşkilində, onun səmərəli və təhlükəsiz ötürülməsini təmin etməkdə əsas rol oynayırlar. Belə ki, kommutatorlar qoşulmuş cihazlardan gələn trafiki təhlil edir və onu yalnız lazımi portlara yönləndirir. Bu, şəbəkə yükünü azaldır və performansını artırır.

SWITCH müxtəlif cihazları əlaqələndirmək üçün müxtəlif sayda portlardan ibarət olur (şəkil 2.2.). Onlar kiçik korporativ şəbəkələr üçün bir neçə portdan, iri korporativ şəbəkələr üçün isə yüzlərlə porta malik ola bilərlər. Bundan əlavə SWITCH administratorlara şəbəkəni konfiqurasiya və nəzarət etməyə imkan verən idarəetməni təmin edir. Buraya Virtual LAN (VLAN) konfiqurasiyası, xidmət keyfiyyətinin idarə edilməsi və digər funksiyalar daxil ola bilər.



Şəkil 2.2. SWITCH konfiqurasiyası

Müasir SWITCH şəbəkəni icazəsiz giriş və hücumlardan qorumaq üçün port əsaslı giriş nəzarəti, cihazın autentifikasiyası və məlumatların şifrələnməsi

kimi müxtəlif təhlükəsizlik mexanizmlərini təmin edir. SWITCH cihazı Ethernet,

Fast Ethernet, Gigabit Ethernet və hətta 10-Gigabit Ethernet və 100-Gigabit Ethernet kimi daha yüksək sürətlər də daxil olmaqla müxtəlif məlumat ötürmə standartlarını dəstəkləyə bilər.

MEDİA ÇEVİRİCİSİ (MEDIA CONVERTER). Media konverter, mis kabel və fiber optik kabel kimi müxtəlif ötürmə mühitləri arasında məlumat siqnallarını çevirmək üçün kompüter şəbəkələrində istifadə olunan bir cihazdır (şəkil 2.3). O, müxtəlif şəbəkə komponentlərinin səmərəli inteqrasiyasına imkan verən müxtəlif növ şəbəkə interfeysləri arasında uyğunluğu təmin edir. Media çeviricisinin əsas funksiyası məlumat siqnallarını bir ötürmə mühitindən digərinə çevirməkdir. Məsələn, o, Ethernet siqnallarını mis kabellərdən fiber optika və ya əksinə çevirə bilər.

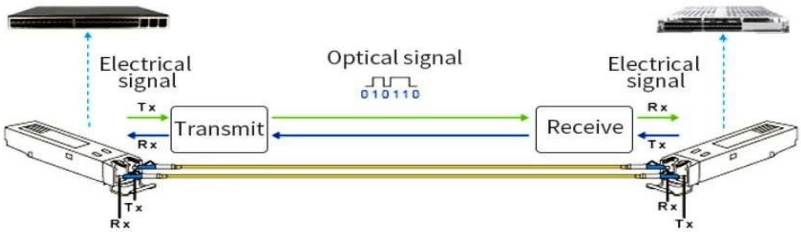
Şəkil 2.3 . MEDİA ÇEVİRİCİSİ (MEDIA CONVERTER)

Media çeviriciləri Ethernet, Fast Ethernet, Gigabit Ethernet kimi müxtəlif standartları və interfeys növlərini, həmçinin müxtəlif növ optik birləşdiriciləri (məsələn, SC, LC) dəstəkləyir. Media çeviricilərindən istifadənin üstünlüklərindən biri onların siqnal ötürmə diapazonunu genişləndirmək qabiliyyətidir. Fiber optik kabellər, məsələn, mis kabellərlə müqayisədə siqnal keyfiyyətini itirmədən məlumatları daha uzun məsafələrə ötürə bilər. Media çeviriciləri adətən sadə interfeysə malikdir və mürəkkəb konfiqurasiyaya ehtiyac olmadan şəbəkədə quraşdırmaq və konfiqurasiya etmək asandır. Media çeviriciləri aktiv şəbəkə infrastrukturunun mühüm elementidir, müxtəlif növ şəbəkə cihazları və məlumat ötürülməsi mediası arasında çeviklik və uyğunluq təmin edir.

SFP ÖTÜRÜCÜSÜ / MODUL (**SFP TRANSCEIVER / MODULE**). SFP (Small Form-factor Pluggable – SFP) modulları kimi tanınan SFP (Small Form-factor Pluggable) ötürücüləri kompüter şəbəkələrində məlumat ötürmək üçün istifadə edilən yığcam və çevik qurğulardır (şəkil 2.4).

Şəkil 2.4. SFP ÖTÜRÜCÜ / MODUL (SFP TRANSCEIVER / MODULE)

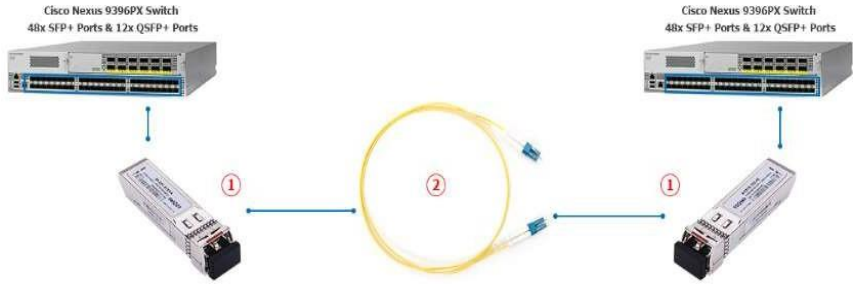
Onlar şəbəkə avadanlıqlarının müxtəlif növ fiber optik və ya mis kabellərə qoşulmasına imkan verən optik modulların bir formasıdır. SFP ötürücüləri şəbəkə tələblərinə uyğun olaraq asanlıqla dəyişdirilə və ya təkmilləşdirilə bilər (şəkil 2.5.).



Şəkil 2.5. SFP ötürücülərinin konfiqurasiyası

SFP ötürücüləri müxtəlif növ lif və mis interfeysləri, o cümlədən müxtəlif Ethernet standartlarını (məsələn, 100BASE-T, 1000BASE-T), Gigabit Ethernet, Fiber Kanal və s. dəstəkləyir. SFP ötürücülərindən istifadə şəbəkənin ötürmə qabiliyyətini və məlumat ötürmə diapazonunu artırmağa imkan verir. Məsələn, onlar Gigabit Ethernet və ya hətta 10-Gigabit Ethernet kimi daha yüksək məlumat sürətlərini dəstəkləyə bilirlər. SFP ötürücülərinin üstünlüklərindən biri onların yerində (cari anda) dəyişdirilə bilməsidir. Bu o deməkdir ki, onlar şəbəkə cihazlarını bağlamaq və ya yenidən yükləməyə ehtiyac olmadan dəyişdirilə və ya avadanlıqlara quraşdırıla bilər. SFP ötürücüləri açarlar, marşrutlaşdırıcılar və digər cihazlar kimi şəbəkə avadanlıqlarında məkandan

səmərəli istifadə etməyə imkan verən kompakt forma faktoruna malikdir. SFP ötürücüləri standart forma faktorundan istifadə etdiyinə görə, onlar müxtəlif istehsalçıların geniş çeşidli şəbəkə avadanlığı ilə uyğun gəlir (şəkil 2.6.).



Şəkil 2.6. SFP ötürücülərinin interfeysi

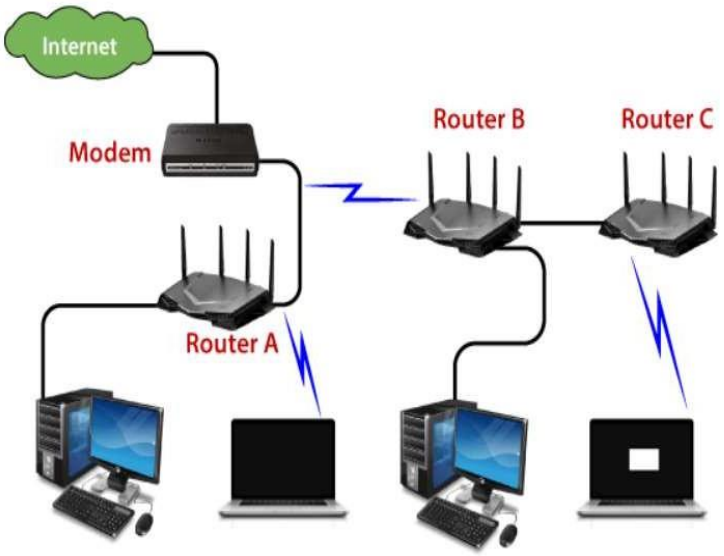
Beləliklə, SFP ötürücüləri bugünkü şəbəkələrdə əsas rol oynayır, müxtəlif növ şəbəkə avadanlığı və məlumat ötürülməsi mediasını birləşdirərkən çeviklik, performans və uyğunluq təmin edir.

MARŞRUTİZATOR (**ROUTER**). Routerlər müxtəlif şəbəkə seqmentləri arasında və ya müxtəlif şəbəkələr arasında məlumat ötürmək üçün istifadə olunan şəbəkə cihazlarıdır (şəkil 2.7).

ROUTER şəbəkə səviyyəsində fəaliyyət göstərir (OSI modelinin şəbəkə səviyyəsi) və məlumat paketinin başlıqlarındakı məlumatlara və şəbəkənin cari vəziyyətinə əsasən məlumatların yönləndirilməsi qərarlarını qəbul edir. Routerin əsas funksiyası məlumat paketlərinin bir şəbəkədən digərinə çatdırılması barədə qərar qəbul etməkdir. Optimal çatdırılma marşrutunu müəyyən etmək üçün paket başlıqlarındakı məlumatlardan (məsələn, IP ünvanları) istifadə edir.

Şəkil 2.7. MARŞRUTİZATOR (ROUTER)

Marşrutlaşdırıcılar şəbəkədə məlumatların çatdırılması üçün ən yaxşı yolları müəyyən etmək üçün OSPF (Open Shortest Path First) və BGP (Border Gateway Protocol) kimi müxtəlif marşrutlaşdırma alqoritmləri və protokollarından istifadə edirlər (şəkil 2.8).



Şəkil 2.8. MARŞRUTİZATOR (ROUTER) konfiqurasiyası

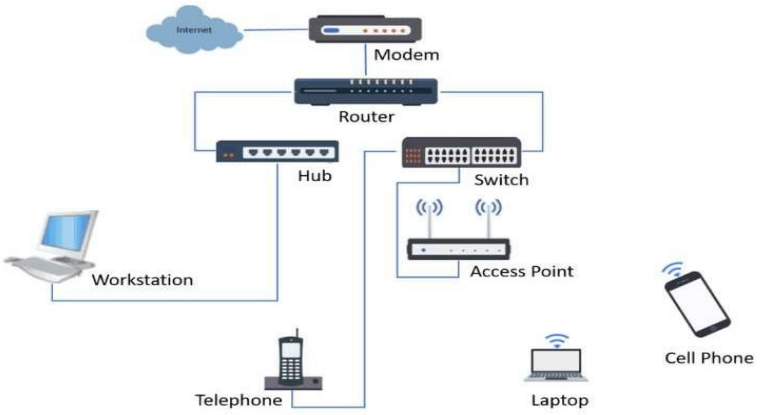
Routerlər şəbəkəni alt şəbəkələr adlanan məntiqi seqmentlərə bölməyə və onlar arasında əlaqə yaratmağa imkan verir. Bu, trafiki idarə etməyə və şəbəkə təhlükəsizliyini yaxşılaşdırmağa kömək edir. Marşrutlaşdırıcılar şəbəkəyə girişi idarə etmək və təhlükəsizliyi təmin etmək üçün IP ünvanları və portlar kimi müxtəlif meyarlar əsasında trafiki süzgəcdən keçirə bilər. Bəzi marşrutlaşdırıcılar İnternet kimi sosial şəbəkə üzərindən uzaq şəbəkələr arasında təhlükəsiz əlaqə yaratmağa imkan verən virtual şəxsi şəbəkələrə (VPN) dəstək verir. Həmçinin şəbəkə performansını və etibarlılığını yaxşılaşdırmaq üçün bir çox mövcud marşrutlar üzrə trafik paylayaraq yük balanslaşdırma xüsusiyyətlərini dəstəkləyir. Beləliklə, marşrutlaşdırıcılar müasir kompüter şəbəkələrinin təşkili və idarə edilməsində, verilənlərin səmərəli marşrutlaşdırılmasını təmin etməkdə və müxtəlif qurğular və şəbəkə seqmentləri arasında əlaqə saxlamaqda əsas rol oynayırlar.

GİRİŞ NÖQTƏLƏRİ (**ACCESS POINTS**). Giriş nöqtələri (AP) simsiz cihazları simli şəbəkəyə qoşmaq üçün simsiz şəbəkələrdə istifadə olunan cihazlardır. Onlar simsiz infrastrukturun qurulmasında, noutbuklar,

smartfonlar və planşetlər kimi mobil cihazlara şəbəkəyə çıxışın təmin edilməsində əsas rol oynayırlar (şəkil 2.9).

Şəkil 2.9. GİRİŞ NÖQTƏLƏRİ (ACCESS POINTS)

Giriş nöqtələri cihazlar və simli infrastruktur arasında simsiz rabitəni təmin edən simsiz şəbəkələr yaradır. Onlar İnternet, lokal serverlər və şəbəkədəki digər cihazlar kimi şəbəkə resurslarına giriş nöqtələrini təmin edir (şəkil 2.10).



Şəkil 2.10. GİRİŞ NÖQTƏLƏRİ (ACCESS POINTS)

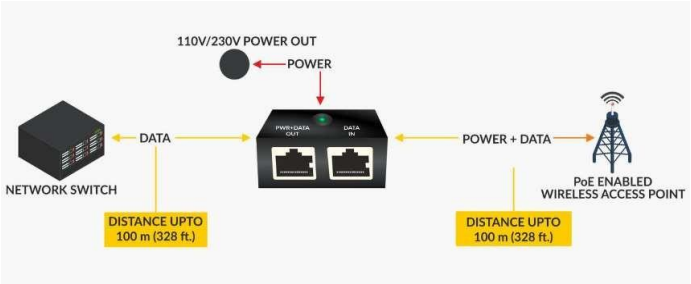
Simsiz şəbəkənin vahid əhatə dairəsini təmin etmək üçün giriş nöqtələri otağın müxtəlif nöqtələrində və ya açıq ərazilərində quraşdırılır. Onlar Wi-Fi siqnalını ötürərək cihazların öz diapazonunda şəbəkəyə qoşulmasına imkan verir. Giriş nöqtələri şəbəkədə simsiz trafikə nəzarəti təmin edir, cihazın şəbəkəyə girişini tənzimləyir və mövcud spektrdən istifadəni optimallaşdırır. Bu, sabit bir əlaqə saxlamağa və şəbəkə sıxlığının qarşısını almağa imkan verir. Bir çox giriş nöqtələri şəbəkəni icazəsiz giriş və hücumlardan qorumaq üçün məlumatların şifrələnməsi (məsələn, WPA2), istifadəçinin autentifikasiyası və trafikin filtrasiyası kimi müxtəlif təhlükəsizlik mexanizmlərini dəstəkləyir. Böyük şəbəkələr bir simsiz infrastruktura birləşdirilə bilən çoxsaylı giriş nöqtələrini əhatə edə bilər. Bu, istifadəçiyə şəbəkə əhatə dairəsini

genişləndirməyə və binalar, ofislər və ya kampuslar kimi böyük ərazilərdə İnternet və şəbəkə resurslarına çıxışı təmin etməyə imkan verir. Bəzi giriş nöqtələri veb interfeysi və ya xüsusi proqram təminatı vasitəsilə şəbəkənin idarə edilməsi və monitorinq imkanlarını təmin edir. Bu, administratorlara şəbəkə parametrlərini konfiqurasiya etməyə, resurs istifadəsinə nəzarət etməyə və rabitə problemlərini həll etməyə imkan verir.

POE İNJEKTORLARI (Power OVER Ethernet injector - POE) elektrik enerjisini və məlumatı bir Ethernet kabeli vasitəsilə şəbəkəyə qoşulmuş güc qurğularına ötürməyə imkan verən cihazdır (şəkil 2.11).

Şəkil 2.11. POE injektoru

POE injektoru Ethernet şəbəkələrində IP kameralar, Wi-Fi giriş nöqtələri, VoIP telefonları və Power over Ethernet (PoE) texnologiyasını dəstəkləyən şəbəkə cihazlarını enerji ilə təmin etmək üçün istifadə olunur. POE injektorunun əsas funksiyası həm məlumatı, həm də elektrik enerjisini eyni Ethernet kabeli üzərindən ötürməkdir (şəkil 2.12).



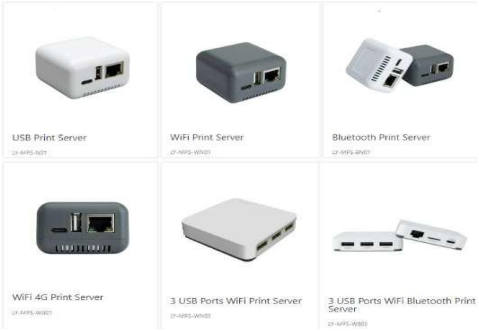
Şəkil 2.12. POE injektorunun konfiqurasiyası

Bu, xüsusilə elektrik prizlərinə çıxışın məhdud olduğu ərazilərdə şəbəkə qurğularının quraşdırılmasını asanlaşdırır. POE injektorundan istifadə şəbəkə

cihazlarını birləşdirmək üçün lazım olan kabellərin sayını azaltmağa imkan verir ki, bu da kabel infrastrukturunun görünüşünü və təşkilini yaxşılaşdırır. POE injektorları şəbəkə cihazlarını quraşdırarkən çeviklik təmin edir, çünki onlar əlavə elektrik rozetkalarının quraşdırılmasını tələb etmir. Bu, əlavə naqillərin çəkilməsinin çətin olduğu yerlərdə xüsusilə faydalıdır.

Ethernet kabeli ilə ötürülə bilən maksimum gücü müəyyən edən IEEE 802.3af və IEEE 802.3at (PoE+) kimi müxtəlif Power over Ethernet standartları mövcuddur. POE injektorları şəbəkə tələblərindən asılı olaraq bu standartlardan birini və ya bir neçəsini dəstəkləyir. POE injektorları kiçik ev şəbəkələrindən tutmuş böyük şəbəkələrə qədər müxtəlif şəbəkə mühitlərində istifadə olunur. Sistem tələblərindən asılı olaraq həm daxili, həm də açıq havada quraşdırıla bilər. Düzgün istifadə edildikdə, POE injektorları Ethernet kabeli üzərindən enerjinin təhlükəsiz ötürülməsini təmin edərək cihazları və istifadəçiləri elektrik şoku riskindən qoruyur. Beləliklə, POE injektorları şəbəkə qurğularını Ethernet infrastrukturu üzərindən enerji ilə təmin etmək üçün rahat və səmərəli həll yolu təqdim edərək, sadələşdirilmiş quraşdırmaya və şəbəkənin yerləşdirilməsi zamanı resursa qənaət etməyə imkan verir.

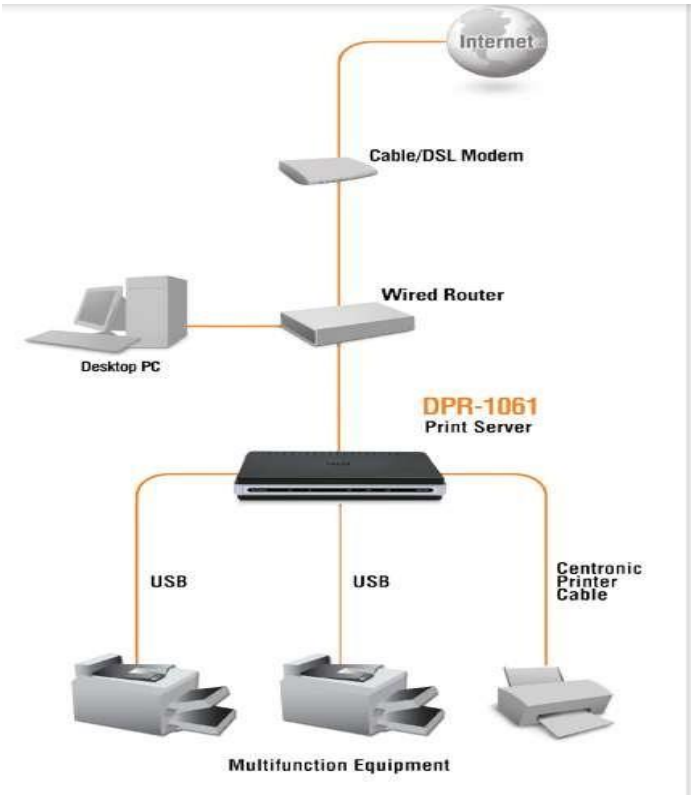
SERVER PRİNTERLƏRİ (PRINT SERVER). Çap serverləri kimi tanınan server printerləri kompüter şəbəkəsi üzərindən çap işlərinin mərkəzləşdirilmiş idarə edilməsini və işlənməsini təmin edən qurğular və ya proqramlardır (şəkil 2.13). Onlar müxtəlif cihazlardan bir neçə istifadəçiyə çap işlərini bir və ya bir neçə şəbəkəyə qoşulmuş printerə göndərməyə imkan verir.



Şəkil 2.13. SERVER PRİNTERLƏRİ (PRINT SERVER)

Çap serverləri şəbəkədəki bütün printerlərin mərkəzləşdirilmiş idarə edilməsini təmin edir. Onlar prioritet və əlçatanlıq parametrlərinə uyğun olaraq şəbəkədəki mövcud printerlər arasında çap işlərini emal edir və paylayır (şəkil 2.14). Çap serverləri printer resurslarını şəbəkədəki bütün istifadəçilərlə

paylaşır. Bu, printerlərdən səmərəli istifadə etməyə və resurs münaqişələrinin qarşısını almağa imkan verir.



Şəkil 2.14. SERVER PRİNTERLƏRİ

Çap serverləri hansı istifadəçilərin xüsusi printerlərdən istifadə etmək səlahiyyətinin olduğunu müəyyən etməklə və həssas məlumatları qorumaq üçün təhlükəsizlik qaydalarını təyin etməklə printerlərə girişi idarə edə bilər. Çap serverləri istifadəçilərə çap işlərini çap növbəsinə təqdim etməyə imkan verir. Bu, çap işinin idarə edilməsini asanlaşdırır və istifadəçilərə işlərinin vəziyyətini izləməyə imkan verir. Bəzi çap serverləri idarəçilərə şəbəkədə printerlərdən istifadəni izləməyə, çap işlərini təhlil etməyə və printerin işini optimallaşdırmağa imkan verən monitorinq və hesabat imkanlarını təmin edir. Çap serverləri inzibatçılara şəbəkənin istənilən yerindən printerləri konfiqurasiya etməyə və nəzarət etməyə imkan verən uzaqdan printer idarəetmə imkanlarını təmin edir. Həmçinin bir çox cihazda universallığı təmin edən simli və simsiz printerlər də daxil olmaqla müxtəlif printer növlərini və əlaqələri dəstəkləyir.

Server printerləri ofislərdə və digər təşkilatlarda çap infrastrukturunun təşkilində, şəbəkə mühitində çap işlərinin səmərəli idarə edilməsi və emalının təmin edilməsində mühüm rol oynayır.

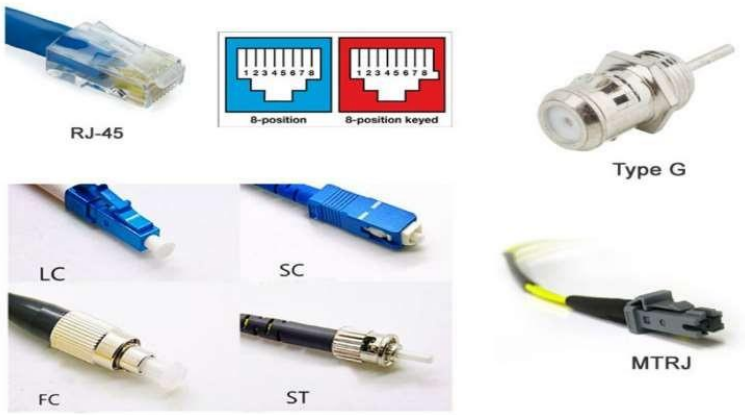
PASSİV ŞƏBƏKƏ CİHAZLARI[10] fiziki səviyyədə sadə siqnal ötürülməsi üçün istifadə olunan avadanlıqdır. Bunlar şəbəkə kabelləri, birləşdiricilər və şəbəkə rozetkaları, təkrarlayıcılar və siqnal gücləndiriciləridir. Passiv şəbəkə cihazlarına aşağıdakılar aiddir:

- Fiber Optik Patch kordları (Fiber Optic Patch cords).
- Fiber optik pigtaillər (Fiber optic Pigtails).
- Birgə qapaqlar (Joint Enclosures).
- LIU qutuları (LIU boxes).
- Şəbəkə Rəfləri (Networking Racks).
- Fiber optik kabellər (Optical Fiber Cables).
- Adapterlər (Adapters).
- Adapter panelləri (Adapter Panels).
- Kabel menecerləri (Cable Managers).
- Enerji paylayıcı qurğular (Power distribution units).
- Üz qapaqları (Face plates).
- UTP patch kordları (UTP Patch cords).
- UTP/STP kabel rulonları (UTP/STP cable rolls).
- Jack/Patch panelləri (Jack/Patch panels).
- Kəsici alətləri (Crimping tools).

Fiber Optik Patch kordları (Fiber Optic Patch cords). Fiber optik patch kordlar, keçidlər, marşrutlaşdırıcılar və ya serverlər kimi şəbəkə avadanlıqlarını fiber optik infrastruktura qoşmaq üçün istifadə edilən passiv şəbəkə cihazlarıdır (şəkil 2.15). Onlar elektrik siqnallarından istifadə etmədən optik liflər vasitəsilə işıq siqnalları şəklində məlumat ötürülməsini təmin edirlər. Bu Patch kordların RJ45, 8P8C, LC, SC, FC, ST, Type G, MTRJ kimi müxtəlif növ bağlayıcılara malikdir və şəbəkənin xüsusi ehtiyaclarından asılı olaraq müxtəlif uzunluqlarda ola bilər. RJ45 kompüterlər, marşrutlaşdırıcılar və açarlar kimi şəbəkə cihazlarını birləşdirmək üçün istifadə edilən standart thernet konnektorudur. Onun 8 pini var və adətən Ethernet kateqoriyalı

[10] Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X.«İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.
Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.

kabellər üçün istifadə olunur. 8P8C "8 pin, 8 mövqe" deməkdir və tez-tez 8 pin olduğu Ethernet konnektorları (məsələn, RJ45) kontekstində istifadə olunur.



Şəkil 2.15. Fiber Optik Patch kordları (Fiber Optic Patch cords)

LC (Lucent Connector) fiber optik kabel konnektorunun bir növüdür. O, kiçikdir və şəbəkə avadanlıqlarında yüksək port sıxlığını təmin edir. LC konnektorları çox rejimli və tək rejimli fiber optik şəbəkələrdə adətən istifadə olunur.

SC (Subscriber Connector) həm də fiber optik kabellər üçün birləşdirici növüdür. LC ilə müqayisədə ölçülərinə görə daha böyükdür və tez-tez çox rejimli və tək rejimli şəbəkələrdə istifadə olunur.

FC (Ferrule Connector) fiber optik kabellər üçün başqa bir bağlayıcı növüdür. Daha təhlükəsiz montaj üçün yivli bir əlaqəyə malikdir və adətən tək rejimli şəbəkələrdə istifadə olunur.

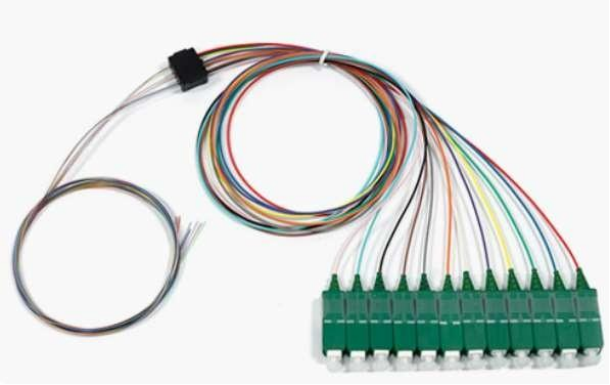
ST (Straight Tip) fiber optik kabellər üçün yüksək səviyyəli birləşdirici növüdür. Onun süngü bağlantısı var və çox rejimli şəbəkələrdə tez-tez istifadə olunur.

G (BS 1363) tipi Böyük Britaniya, Honq-Konq, İrlandiya və digər ölkələrdə istifadə olunan standart elektrik bağlayıcı növüdür. Elektrik hissələri ilə təsadüfi təmasdan qorunma təmin edir və adətən AC çıxışları üçün istifadə olunur.

MTRJ (Mechanical Transfer Registered Jack) iki lifi bir konnektorda birləşdirən kompakt fiber optik kabel konnektorudur. Tez-tez yerli şəbəkələrdə (LAN) və telekommunikasiya şəbəkələrində istifadə olunur.

Bu bağlayıcıların və növlərin hər biri şəbəkə və elektrik sistemlərində öz xüsusiyyətlərinə və tətbiqlərinə malikdir.

Fiber optik pigtaillər (Fiber optic Pigtails). Fiber optik pigtaillər, bir ucunda bir konnektor quraşdırılmış fiber optik kabelin qısa parçalarıdır (şəkil 2.16).



Şəkil 2.16. Fiber optik pigtaillər (Fiber optic Pigtails)

Onlar fiber optik kabelləri patç (patch) panellər, splitterlər kimi avadanlıqlara birləşdirmək və müxtəlif növ fiber optik kabelləri birləşdirmək üçün istifadə olunur. Pigtaillərin adətən bir ucunda LC, SC, ST, FC və ya digər fiber optik bağlayıcılar kimi birləşdiricilər quraşdırılır. Pigtaillərin uzunluğu şəbəkənin xüsusi ehtiyaclarından asılı olaraq bir neçə santimetrdən bir neçə metrə qədər dəyişə bilər. Pigtaillər şəbəkə tələblərindən asılı olaraq tək rejimli və ya çox rejimli lifdən hazırlana bilər. Adətən pigtaillərdə lifləri mexaniki zədələrdən qorumaq üçün plastik və ya rezindən hazırlanmış qoruyucu örtüklər olur. Müxtəlif növ lifləri və ya bağlayıcıları müəyyən etməyə kömək etmək üçün pigtaillərə tez-tez müxtəlif rənglər verilir.

Fiber optik pigtaillər fiber optik məlumat şəbəkələrində mühüm komponentdir, fiber optik kabel və şəbəkə avadanlığı arasında etibarlı və rahat əlaqə təmin edir.

Birgə korpus (Joint Enclosures). "Birgə korpus" müxtəlif kontekstlərdə istifadə oluna bilən termindir, lakin çox vaxt şəbəkə və ya telekommunikasiya sistemlərində müxtəlif avadanlıqları və ya bir-birini birləşdirən cihazları yerləşdirmək və qorumaq üçün nəzərdə tutulmuş korpuslara və ya şkaflara aiddir (şəkil 2.17). Bu qapaqlar marşrutlaşdırıcılar, açarlar, patç panellər və

serverlər kimi şəbəkə avadanlıqlarını yerləşdirmək üçün istifadə olunur. Onlar avadanlığın tozdan, nəmdən və xarici zədələrdən qorunmasını təmin edir, həmçinin texniki xidmət üçün girişi asanlaşdırır.

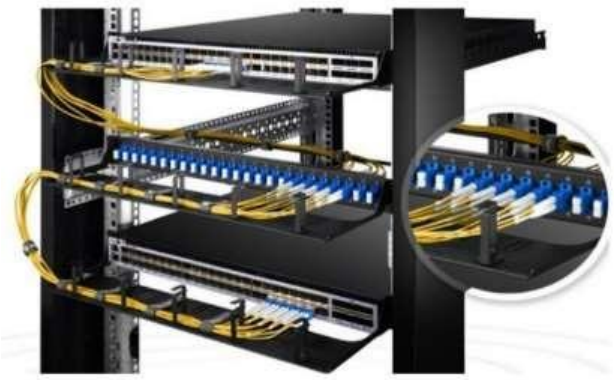
Şəkil 2.17. Birgə korpus (Joint Enclosures)

Bu qapaqlar fiber optik paylayıcı panelləri, işıq borularını və digər fiber optik avadanlıqları yerləşdirmək üçün nəzərdə tutulmuşdur. Onlar adətən fiber optik əlaqələrin təşkili və qorunması üçün xüsusi elementlərə malikdirlər. Bu qapaqlar rozetkalar, açarlar və paylayıcı lövhələr kimi elektrik avadanlıqlarını yerləşdirmək üçün istifadə olunur. Bu korpuslar məlumat kommunikasiya avadanlığı, telefon sistemləri və video konfrans avadanlığı kimi telekommunikasiya avadanlıqlarını yerləşdirmək üçün nəzərdə tutulmuşdur. Onlar təhlükəsizlik və avadanlıqlara giriş asanlığını təmin edir. Birgə qapaqların ümumi məqsədi şəbəkə və ya telekommunikasiya sistemlərində istifadə olunan müxtəlif avadanlıq və ya birləşdirici qurğuların mühafizəsini, təşkilini və onlara çıxışın asanlığını təmin etməkdir.

LIU qutuları (LIU boxes). LIU açıq liflərin birləşdirilməsi, optik kabellərin çəkilməsi və pigtaillərin saxlanması və idarə edilməsi üçün istifadə olunan lif birləşdirmə vahididir. Birgə korpus (şəkil 2.17) kimi LIU qutuları da, optik lif birləşmələrinin tozdan, nəmdən və mexaniki zədələrdən qorunmasını, eləcə də texniki xidmət üçün girişin asanlığını təmin edir (şəkil 2.18).

Patch cord adətən dörd cüt naqildən ibarət yüksək keyfiyyətli çoxnüvəli kabeldir. Onun hər iki ucunda modul konnektorlar (məsələn, Ethernet üçün

RJ45) var və kompüterlər, marşrutlaşdırıcılar və ya switch kimi şəbəkə cihazlarını aktiv portlara qoşmaq üçün istifadə olunur.



Şəkil 2.18. LIU qutuları

Şəbəkə rəfləri (Networking Racks). Şəbəkə rəfləri, tez-tez avadanlıq rəfləri və ya server rəfləri də adlandırılır. Şəbəkə rəfləri strukturlaşdırılmış kabel sistemlərində şəbəkə və server avadanlıqlarını yerləşdirmək və təşkil etmək üçün nəzərdə tutulmuş metal konstruksiyalardır (şəkil 2.19).

Şəkil 2.19. Şəbəkə rəfləri (Networking Racks)

Şəbəkə rəfləri əksər server və şəbəkə avadanlıqlarına uyğun olmaq üçün adətən 19 düym genişlik kimi standart ölçülərdə olur. Yerləşdirilməsi lazım

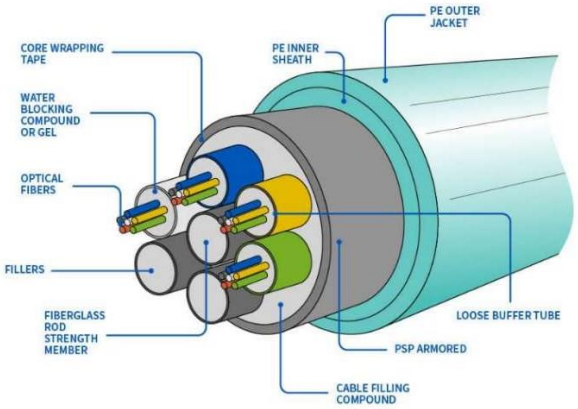
olan avadanlığın miqdarından asılı olaraq onlar həmçinin 24U, 42U, 36U və s. kimi müxtəlif hündürlüklərdə ola bilər. Rəflər adətən davamlı poladdan hazırlanır və kabelləri gücləndirmək və təşkil etmək üçün əlavə elementlərlə təchiz oluna bilər. Rəflər adətən serverləri, açarları, patç panelləri, gərginlik stabilizatorlarını və digər avadanlıqları quraşdırmaq üçün bir sıra montaj avadanlıqları ilə birlikdə təqdim olunur. Onlar həmçinin avadanlığın asan quraşdırılması və saxlanması üçün relsləri də əhatə edə bilər. Şəbəkə rəfləri şaquli və üfüqi kabel menecerləri, kabel rəfləri və kabel kanalları kimi kabel idarəetmə seçimlərini təmin edir. Bu, kabel tıxanmasını yüngülləşdirməyə kömək edir, yaxşı ventilyasiya təmin edir və texniki xidmət üçün kabellərə girişi asanlaşdırır. Bəzi şəbəkə rəfləri server avadanlığının lazımi ventilyasiyasını və soyumasını təmin etmək üçün havalandırma dəlikləri və ya ventilyatorlarla təchiz oluna bilər ki, bu da həddindən artıq istiləşmənin qarşısını alır və avadanlıqların etibarlılığını artırır. Bəzi rəf modellərində qapıların bağlanması və kilidlənməsi imkanları, həmçinin avadanlıqları icazəsiz girişdən qorumaq üçün çıxarıla bilən yan panellər ola bilər.

Fiber optik kabellər (Optical Fiber Cables). Fiber optik kabellər işıq siqnallarını ötürən nazik şüşə və ya plastik liflərdən ibarət məlumat ötürmə mühitidir. Onlar telekommunikasiya şəbəkələrində, internet xidmət provayderlərində, müəssisə rabitə şəbəkələrində, tibbi avadanlıqlarda və uzun məsafələrə yüksək sürətli məlumat ötürülməsi tələb olunan digər sahələrdə geniş istifadə olunur (şəkil 2.20). Fiber optik kabel nüvədən (mərkəzi hissə), örtükdən (nüvəni əhatə edən) və qoruyucu gödəkçədən (xarici səviyyə) ibarətdir. Nüvə adətən təmiz şüşə və ya plastikdən hazırlanır və işıq siqnalının ötürülməsinə cavabdehdir. Qabıq və ya qoruyucu qabıq nüvəni mexaniki zədələrdən və xarici təsirlərdən qorumağa xidmət edir. Fiber optik kabellər işıq siqnallarını necə ötürdüklərindən asılı olaraq tək rejimli və ya çox rejimli ola bilər.

Tək rejimli liflər işığı bir istiqamətə ötürmək üçün nəzərdə tutulmuşdur və daha dar bir nüvəyə malikdir, bu da daha uzun məsafələrdə daha sürətli məlumat ötürülməsinə imkan verir. Multimod lifləri daha geniş nüvəyə malikdir və işığı bir çox istiqamətə ötürə bilir, bu da onları daha qısa məsafələr üçün uyğun edir. Fiber optik kabelləri bir-birinə və ya aktiv avadanlıqlara qoşmaq üçün LC, SC, ST, FC və başqaları kimi müxtəlif növ bağlayıcılardan istifadə olunur.

Fərqli bağlayıcılar xüsusi şəbəkə ehtiyacları üçün optimallaşdırıla bilən müxtəlif dizayn və xüsusiyyətlərə malikdir. Fiber optik kabellər uzun

məsafələrə yüksək sürətli məlumat ötürmək üçün geniş istifadə olunur. Onlar yüksək ötürmə qabiliyyətinə, elektromaqnit müdaxiləsinə qarşı toxunulmazlığa, uzun məsafələrdə daha az siqnal itkisinə malikdir və mis kabellərə nisbətən məlumatların tutulmasından daha çox qorunmasını təmin edir. Fiber optik kabellərin quraşdırılması xüsusi avadanlıq və bacarıqlar tələb edir.



Şəkil 2.20. Fiber optik kabellər (Optical Fiber Cables)

Onlar yeraltı, binaların divarları boyunca, dənizdə və digər şəraitdə quraşdırıla bilər. Fiber optik kabelə texniki qulluq adətən şəbəkənin etibarlı işləməsini təmin etmək üçün əlaqələrin yoxlanılmasını və birləşdiricilərin tənzimlənməsini əhatə edir. Fiber optik kabellər müasir telekommunikasiya şəbəkələrinin mühüm tərkib hissəsidir, uzun məsafələrə sürətli və etibarlı məlumat ötürülməsini təmin edir.

Fiberoptik adapterlər (Adapters)[11]. Optik birləşdiricilər kimi tanınan fiber optik adapterlər iki fiber optik kabeli və ya komponenti birləşdirmək üçün istifadə olunan cihazlardır. Onlar müxtəlif tipli və ya eyni tipli optik bağlayıcılar arasında etibarlı və dəqiq əlaqə yaratmağa imkan verir.

Fiber optik adapterin hər iki ucundakı birləşdirici növü fiber adapterin əsas atributudur. Fiber adapterin hər iki ucundakı bağlayıcılara görə eyni və ya fərqli fiber optik adapter növlərinə ayrılır. Hər iki ucu da eyni olan fiber optik adapterin strukturu şəkil (şəkil 2.21)-də göstərilmişdir.

[11] https://www.howtonetwork.com/comptia-network-study-guide-free/

Şəkilə əsasən eyni ucluqlu fiber optik adapterlərin aşağıdakı növləri mövcuddur.

- LC-LC
- SC-SC
- ST-ST
- FC-FC
- MPO-MPO

Şəkil 2.21. Eyni ucluqlu fiber optik adapterlər

Müxtəlif ucluqlu fiber optik adapterlərin strukturu şəkil 2.22-də təsvir olunmuşdur. Şəkilə əsasən müxtəlif ucluqlu fiber optik adapterlərin aşağıdakı növləri mövcuddur.

- LC-SC
- LC-ST
- LC-FC
- SC-ST
- SC-FC
- FC-ST

Adapterlər adətən birləşmələri tozdan, nəmdən və mexaniki zədələrdən qoruyan plastik və ya metal korpusa malikdir. Korpusun içərisində minimum siqnal itkisini təmin etmək üçün optik liflərin dəqiq yerləşdirilməsini təmin edən dəqiq kalibrlənmiş mexanizmlər mövcuddur. Fiber Optik Adapterlər telekommunikasiya şəbəkələrində, lokal şəbəkələrdə (LAN), məlumat mərkəzlərində, telekommunikasiya otaqlarında və fiber optik kabellərin və ya komponentlərin bir-birinə qoşulması tələb olunan digər yerlərdə geniş istifadə olunur.

Fiber optik adapterlərin quraşdırılması optik birləşdiricilərin düzgün qoşulmasını və minimum siqnal itkisini təmin etmək üçün diqqətlilik və

dəqiqlik tələb edir. Onlar optik patch panellərə, LIU qutularına, avadanlıq panellərinə və ya digər cihazlara quraşdırıla bilər. Kabel sistemlərinin identifikasiyası və idarə edilməsinin asanlığı üçün fiber optik adapterlər çox vaxt xüsusi standartlara və rəng kodlarına uyğun olaraq işarələnir və rənglənir. Fiber optik adapterlər fiber optik şəbəkələrdə etibarlı və səmərəli birləşmələrin təmin edilməsində mühüm rol oynayır, məlumatların uzun məsafələrdə təhrifsiz və itkisiz ötürülməsini təmin edir.

Şəkil 2.22. Müxtəlif ucluqlu fiber optik adapterlər

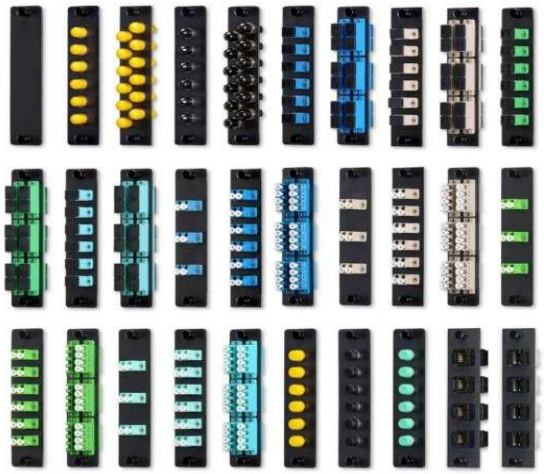
Adapter panelləri (Adapter Panels)[12]. Bağlantı panelləri və ya yamaq panelləri kimi də tanınan adapter panelləri fiber optik şəbəkələrin əsas komponentidir. Onlar fiber optik kabellər və açarlar və ya marşrutlaşdırıcılar kimi aktiv şəbəkə avadanlığı arasında əlaqələri təşkil etmək və idarə etmək üçün nəzərdə tutulmuşdur. Adapter panelləri adətən optik adapterləri qəbul etmək üçün nəzərdə tutulmuş yuva və ya deşik sıraları olan metal və ya plastik çərçivəyə malikdir (şəkil 2.23).

Yuvalar çox vaxt idarə və xidmət üçün rəng və ya işarələrlə asanlıqla müəyyən edilə bilən qruplara bölünür. Adapter panelləri müxtəlif ölçülərdə və konfiqurasiyalarda, o cümlədən panel başına müxtəlif sayda portlarda mövcuddur. Sahə sıxlığı panel sahəsinə düşən yuvaların sayı ilə müəyyən edilir

[12] https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

ki, bu da müəyyən bir şəbəkə infrastrukturu üçün ən uyğununu seçməyə imkan verir.

Adapter panelləri LC, SC, ST, FC və başqaları kimi müxtəlif növ optik birləşdiriciləri dəstəkləyə bilər. Bu, müxtəlif növ fiber optik kabellər və avadanlıqlarla çeviklik və uyğunluğu təmin edir. Adapter panelləri adətən şəbəkə şkafında və ya rəfdə quraşdırılır.



Şəkil 2.23. Adapter panelləri

Kabel menecerləri (Cable Managers). Kabel menecerləri rəflərdə, şkaflarda və kabellərin istifadə olunduğu digər yerlərdə kabelləri təşkil etmək və idarə etmək üçün nəzərdə tutulmuş cihazlardır (şəkil 2.24).

Şəkil 2.24. Kabel menecerləri(Cable Managers).

Kabel menecerlərinin[13] əsas funksiyası naqillərin dolaşıqlığını azaltmaq üçün kabellərin təşkili və idarə edilməsini təmin etməkdir. Onlar şəbəkəyə texniki qulluq və yenidən konfiqurasiya üçün onlara daxil olmağı asanlaşdıran strukturlaşdırılmış kabel sxemini təmin edir. Kabel menecerləri adətən şəbəkə avadanlıqlarını yerləşdirmək üçün istifadə olunan şaquli və ya üfüqi rəflərdə quraşdırılır. Onlar rəfə etibarlı bir əlavə təmin edən bağlayıcılar və ya montajlar istifadə edərək quraşdırıla bilər. Kabel menecerlərinin ən çox şaquli və üfüqi modellərindən istifadə olunur. Şaquli kabel menecerinin strukturu şəkil 2.25-də təsvir olunmuşdur.

Şəkil 2.25. Şaquli Kabel meneceri

Üfuqi kabel menecerinin strukturu şəkil 2.26-da təsvir olunmuşdur.

Şəkil 2.26. Üfuqi kabel meneceri

13 https://www.howtonetwork.com/comptia-network-study-guide-free/

Hər növ kabel meneceri şəbəkənin xüsusi ehtiyaclarından asılı olaraq seçilə bilər. Etibarlılıq və davamlılığı təmin etmək üçün kabel menecerləri adətən metal və ya plastik kimi davamlı materiallardan hazırlanır. Onların müxtəlif dizayn xüsusiyyətləri ola bilər, məsələn, kabellərin yönləndirilməsi üçün xüsusi kanallar, qoruyucu qabıqlar və ya kabellərin bərkidilməsi üçün üzüklər və s. Bəzi kabel menecerləri kabel sistemlərinin yaxşı ventilyasiyasını və soyumasını təmin edən ventilyasiya və ya digər dizayn xüsusiyyətlərinə malik ola bilər ki, bu da həddindən artıq istiləşmənin qarşısını alır və avadanlıqların etibarlılığını qoruyur. Kabel menecerləri kabellərin və cihazların müəyyən edilməsini asanlaşdırmaq üçün etiketləmə prinsipindən istifadə edirlər. Kabel menecerləri şəbəkə infrastrukturunun mühüm hissəsidir, nizamlı və etibarlı kabel idarəetməsini təmin edir ki, bu da şəbəkənin səmərəli işləməsi və avadanlıqların saxlanılması üçün vacibdir.

Enerji paylayıcı qurğular (Power distribution units)[14]. Paylayıcı qurğular şəbəkə və ya sistemdəki müxtəlif cihazlar və ya komponentlər arasında siqnalları və ya resursları paylamaq üçün istifadə olunan avadanlıqdır (şəkil 2.27).

Şəkil 2.27. Enerji paylayıcı qurğular (Power distribution units)

[14] https://www.howtonetwork.com/comptia-network-study-guide-free/

Onlar trafikin, məlumatların, enerjinin və ya digər resursların idarə edilməsində və nəzarətində mühüm funksiyanı yerinə yetirirlər. Yamaq panelləri şəbəkə kabel əlaqələrini təşkil etmək və idarə etmək üçün istifadə olunan cihazlardır. Onlar adətən şəbəkə rəflərində quraşdırılır və açarlar və ya marşrutlaşdırıcılar kimi şəbəkə avadanlığı arasında kabelləri birləşdirmək üçün rahat bir mexanizm təqdim edir. Çarpaz panellər telekommunikasiya sistemlərində müxtəlif kanallar və ya cihazlar arasında siqnalları birləşdirmək və dəyişdirmək üçün istifadə olunur. Onlar adətən məlumat axınına və telefon əlaqələrinə nəzarət etmək üçün rabitə mərkəzlərində istifadə olunur.

Üz qapaqları (Face plates). Üz plitələri və ya montaj plitələri kimi də tanınan üz lövhələri müxtəlif portları və birləşdiriciləri təşkil etmək üçün rəflərə, divar qutularına və ya panellərə quraşdırılmaq üçün istifadə olunan komponentlərdir. Onlar şəbəkə və ya audio-video konnektorlara rahat girişi təmin edir və evlər, ofislər, sinif otaqları və s. kimi müxtəlif yerlərdə xüsusi əlaqə nöqtələri yaratmaq üçün istifadə edilə bilər (şəkil 2.28).

Şəkil 2.28. Üz qapaqları (Face plates)

UTP patch kordları (UTP Patch cords). UTP (Unshielded Twisted Pair) yamaq şnurları Ethernet şəbəkəsindəki cihazları birləşdirmək üçün istifadə edilən şəbəkə kabellərinin ən çox yayılmış növlərindən biridir (şəkil 2.29). UTP yamaq şnurlarında keçiricilərin ətrafında qoruyucu və ya qoruyucu örtük yoxdur. Bunun əvəzinə keçiricilər bir-birinə bükülmüş cüt keçiricilərdir ki, bu da elektromaqnit müdaxiləsinin təsirlərini yüngüllətməyə kömək edir və cütlər arasında qarşılıqlı əlaqəni azaltmağa xidmət edir.

UTP patch kordları Cat5e, Cat6, Cat6a və s. kimi kateqoriyalara təsnif edilə bilər. Bu kateqoriyalar maksimum məlumat ötürmə qabiliyyətini və

diapazonunu müəyyənləşdirir. Məsələn, Cat5e 100 metrə qədər məsafədə 1000

Mbit/s-ə qədər məlumat ötürülməsini təmin edir. UTP patch kordları adətən RJ45 kimi hər iki ucunda modul bağlayıcılarla təchiz edilir. Bu bağlayıcılar kompüterlər, açarlar, marşrutlaşdırıcılar və digər avadanlıqlar kimi şəbəkə cihazlarına asan qoşulma təmin edir. UTP patch kordları ofis və ev şəbəkələrində, məlumat mərkəzlərində, server otaqlarında, həmçinin kommersiya və sənaye şəbəkələrində geniş istifadə olunur.

Şəkil 2.29. UTP patch kordları (UTP Patch cords)

Onlar şəbəkə avadanlığını Ethernet şəbəkəsinə qoşmaq üçün rahat və etibarlı üsul təqdim edirlər. UTP patch kordları şəbəkədəki kabelləri çeşidləməyə və müəyyən etməyə kömək edən mavi, boz, qara və s. kimi müxtəlif rənglərdə verilə bilər. Onlar bir neçə santimetrdən bir neçə metrə qədər və ya daha çox olan müxtəlif uzunluqlarda da mövcuddur.

UTP patç kordları Ethernet şəbəkəsində cihazları birləşdirən etibarlı və rahat vasitədir və müasir şəbəkə infrastrukturlarında geniş istifadə olunur.

UTP/STP kabel rulonları (UTP/STP cable rolls). UTP (Unshielded Twisted Pair) və STP (Shielded Twisted Pair) kabel rulonları ofislər, evlər, məlumat mərkəzləri və digər binalar kimi müxtəlif yerlərdə şəbəkə əlaqələri yaratmaq üçün istifadə edilə bilən şəbəkə kabellərinin sarılmış makaralarıdır (şəkil 2.30).

UTP (ekranlaşdırılmamış kabel) kabelində keçiricilərin ətrafında qoruyucu qalxan yoxdur. Xarici müdaxiləni və çarpışmanı azaltmaq üçün bir-birinə bükülmüş cüt keçiricilərdən ibarətdir. UTP kabelləri tez-tez Cat5e, Cat6, Cat6a və s. kimi ofis və ev Ethernet şəbəkələrində istifadə olunur. Bu kabellər əksər şəbəkə proqramları üçün asan quraşdırma və sərfəli həllər təmin edir.

Şəkil 2.30. UTP/STP kabel rulonları (UTP/STP cable rolls)

STP (ekranlaşdırılmış Kabel) kabelinin elektromaqnit müdaxiləsindən və xarici təsirlərdən qorunması üçün keçiricilərin ətrafında qoruyucu qalxan var. Ekranlama müdaxiləyə qarşı daha çox qorunma təmin edir və sənaye qurğuları və ya yüksək avadanlıq sıxlığı olan ərazilər kimi yüksək səviyyəli elektromaqnit müdaxiləsi olan mühitlərdə xüsusilə faydalı ola bilər. STP kabelləri tez-tez məlumat mərkəzləri kimi daha tələbkar şəbəkə mühitlərində istifadə olunur, burada xarici müdaxilə olmadan etibarlı məlumat ötürülməsini təmin etmək vacibdir. UTP və STP kabel rulonları müxtəlif kateqoriyalarda (məsələn, Cat5e, Cat6, Cat6a) və müxtəlif uzunluqlarda mövcud ola bilər ki, bu da istifadəçilərin xüsusi ehtiyaclarından və şəbəkə layihəsi tələblərindən asılı olaraq ən uyğun variantı seçməyə imkan verir.

Jack/Patch panelləri (Jack/Patch panels). Jack/Patch panelləri şəbəkə infrastrukturunun əsas komponentləridir, şəbəkə kabel əlaqələrini təşkil etmək və idarə etmək üçün istifadə olunur (şəkil 2.31).

Şəkil 2.31. Jack/Patch panelləri (Jack/Patch panels)

Jaklar divar qutularında, çərçivələrdə və ya digər cihazlarda quraşdırılmış bağlayıcılardır. Onlar kompüterlər, telefonlar, təhlükəsizlik kameraları və digər avadanlıqlar kimi şəbəkə cihazlarını şəbəkə kabellərinə fiziki olaraq qoşmaq üçün istifadə olunur. İstifadə olunan şəbəkə standartından (məsələn, Ethernet üçün RJ45 və ya telefon xətləri üçün RJ11) və kabel standartından (məsələn, Cat5e, Cat6, Cat6a) asılı olaraq jaklar müxtəlif növ ola bilər. Patch panelləri şəbəkə bağlantılarını təşkil etmək və idarə etmək üçün cərgələrin quraşdırıldığı cihazlardır. Bu panellər şəbəkə kabellərini mərkəzləşdirilmiş şəkildə birləşdirmək üçün adətən şəbəkə rəflərində quraşdırılıraraq, switch və ya marşrutlaşdırıcılar kimi aktiv şəbəkə avadanlıqlarına qoşula bilər. Patch panelləri tək (bir növ jak ehtiva edən) və ya hibrid (müxtəlif tipli jak ehtiva edən) ola bilər. Onlar şəbəkə bağlantılarını idarə etmək üçün rahat mexanizm təqdim edərək, şəbəkəni saxlamağı və yenidən konfiqurasiya etməyi asanlaşdırır. Tipik olaraq, şəbəkə kabelləri (yamaq şnurları) patç panelindəki jaklara birləşdirilir, sonra patch paneldən olan kabellər şəbəkə əlaqələrinin rahat və mütəşəkkil paylanmasını təmin edərək aktiv şəbəkə avadanlığına birləşdirilir.

Kəsici, sıxıcı alətləri (Crimping tools). Kəlbətin alətləri etibarlı və davamlı əlaqələr yaratmaq üçün şəbəkə kabellərinin (məsələn, RJ45) uclarına birləşdiricilər quraşdırmaq üçün istifadə olunan alətlərdir (şəkil 2.32).

Şəkil 2.32. Kəsici, sıxıcı alət (Crimping tools)

Krimper şəbəkə kabellərinin uclarına birləşdiricilər quraşdırmaq üçün istifadə edilən əsas kəsici, sıxıcı alətidir. Bu alət etibarlı əlaqəni təmin etmək üçün vacib olan bağlayıcının vahid və yüksək keyfiyyətli sıxılmasını təmin edir. Naqil soyma alətləri kabelin xarici örtüyünü çıxarmaq və konnektoru bükməzdən əvvəl keçiriciləri aşkar etmək üçün istifadə olunur. Konnektorla düzgün əlaqəni təmin etmək üçün keçiricilərdən izolyasiyanın dəqiq və

təhlükəsiz çıxarılmasını təmin edir. Kəsici, sıxıcı alətlər şəbəkə kabelinin və konnektorun quraşdırılması prosesinin mühüm tərkib hissəsidir və bu alətlərin düzgün seçilməsi və istifadəsi etibarlı, keyfiyyətli şəbəkə bağlantısını təmin etməyə kömək edir.

OSI VƏ TCP/ IP MODELI

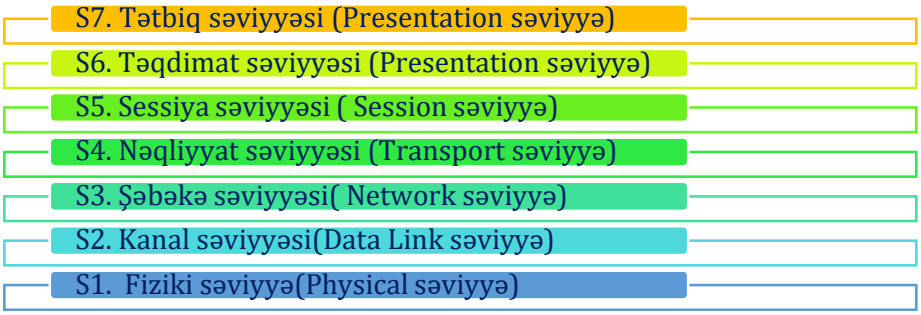
Yaranma tarixi. İlk kompüter şəbəkələri 1960-cı illərin sonlarında universitetlərdə, dövlət qurumlarında və hərbidə yaranmağa başladı. Onlar əsasən özəl şirkətlər tərəfindən hazırlanmış və yalnız öz avadanlıqları üçün nəzərdə tutulmuşdur. Bu şirkətlərdən ən məşhuru SNA (Systems Network Architecture) çoxsəviyyəli şəbəkə arxitekturasını təklif edən Amerikanın IBM korporasiyası idi. Eyni zamanda ABŞ Müdafiə Nazirliyi özünün ARPANET (Advanced Research Projects Agency Network)[15] şəbəkəsini işə saldı. Lakin bütün bu inkişaflarda fərqli şəbəkələrdə yerləşən müxtəlif istehsalçıların kompüterlərinin bir-biri ilə əlaqə saxlamasına imkan verməyən əsas çatışmazlıqlar mövcud idi. Buna görə də, 1977-ci ildə ISO (International Organization for Standardization) qeyri-hökumət təşkilatı universal açıq şəbəkə konsepsiyasını yaratmaq üçün Çarlz Baxmanın rəhbərliyi altında ABŞ, Böyük Britaniya və Fransadan bir qrup alimi cəlb etdi. Standartın yaradılması kompüter avadanlığı və telefon istehsalçıları, tədqiqadçılar, agentliklər, müxtəlif ölkələrin nazirlikləri və hökumətləri tərəfindən fəal şəkildə dəstəkləndi. Yeddi illik gərgin işdən sonra, 1984-cü ildə elm adamları nəhayət, ISO 7498 standartı və ya Açıq Sistemlərin Qarşılıqlı Əlaqəsi üçün Əsas Referans Modeli – OSI (Open Systems Interconnection) kimi tanınan sənədi nəşr etdilər. OSI modeli proqram təminatından tutmuş aparat komponentlərinə qədər bütün növ şəbəkə rabitəsini təsvir edir.

OSI lokal və qlobal şəbəkələrdəki cihazların məlumat mübadiləsini, şəbəkə marşrutlarının necə qurulduğunu və bütün cihazların məlumat ötürmə yolu boyunca necə qarşılıqlı əlaqədə olduğunu dəqiq təsvir edir. OSI modelinə

[15] Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.
Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. М.: Форум, Инфра-М, 2017. 416 с.
https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

xas olan prinsiplər bu və ya digər şəkildə şəbəkəyə qoşulmuş hər bir cihazda - kompüterlərdə, telefonlarda, planşetlərdə, şəbəkə printerlərində, təhlükəsizlik kameralarında, ağıllı ev komponentlərində, marşrutlaşdırıcılarda, modemlərdə informasiyanın mübadiləsi prosesinin səmərəli, etibarlı şəkildə ötürülməsinə xidmət edir.

OSI Modelinin səviyyələri[16]. OSI modeli məlumat ötürülməsi zamanı hər biri xüsusi funksiyaları yerinə yetirən yeddi səviyyədən ibarətdir. OSI modelinin səviyyələri şəkil 2.33-də təsvir olunmuşdur.



Şəkil 2.33. OSI modelinin səviyyələri

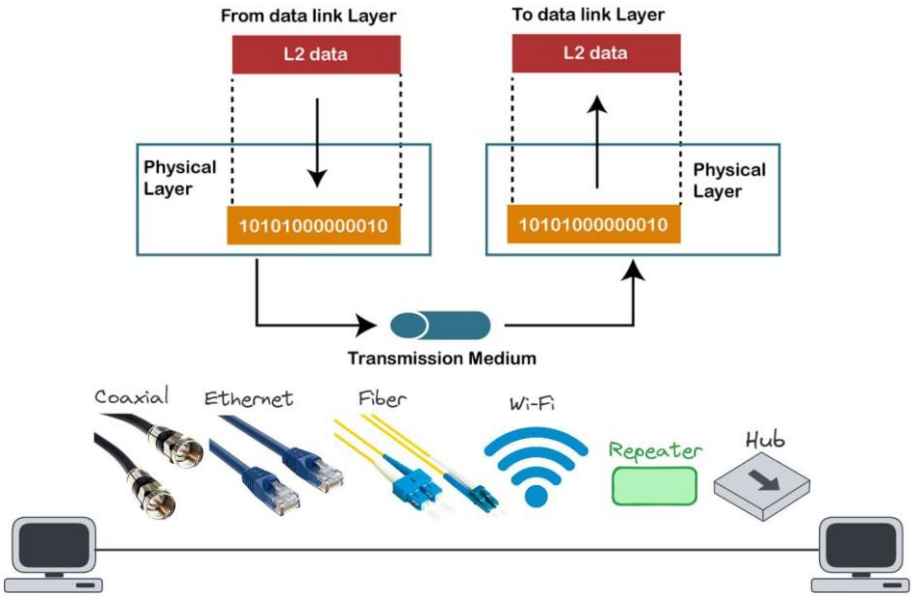
Beləliklə, OSI modelinin səviyyələri və işləmə prinsipinin əsas xarakterik xüsusiyyətləri cədvəl 2.1-də təsvir olunmuşdur.

Cədvəl 2.1.

OSİ səviyyələri		PDU	Xüsusiyyətlər		
7	Tətbiq səviyyəsi	Verilənlər	HOST	↑ Dekapsulyasiya (S1-S7)	↓ İnkapsulyasiya (S7-S1)
6	Təqdimat səviyyəsi				
5	Seans səviyyəsi				
4	Nəqliyyat səviyyəsi	Seqment Dataqram			
3	Şəbəkə səviyyəsi	Paket	MEDİA		
2	Kanal səviyyəsi	Kadr			
1	Fiziki səviyyə	Bit			

Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.

Fiziki səviyyə (S1) fiziki qurğular, aparatlar arasında fiziki siqnalların mübadiləsin yerinə yetirir (şəkil 2.34). Məlumdur ki, kompüter avadanlığı şəklin nə olduğunu və ya onun üzərində nə təsvir olunduğunu başa düşmür; aparat istənilən təsviri yalnız sıfırlar və birlər toplusu, yəni bitlər şəklində başa düşür. Hər səviyyənin öz Vahid Məlumat Protokolu (Protocol Data Unit - PDU) mövcuddur ki, bu da səviyyəni başa düşülən formada təqdim olunmasına imkan verir. Təmiz məlumatlarla iş yalnız S5-S7 səviyyələrində yerinə yetirilir. Fiziki səviyyənin cihazları bitlər üzərində işləyir. Onlar kabellərlə, məsələn, optik lif vasitəsilə və ya kabelsiz şəkildə, məsələn, Bluetooth, Wi-Fi, GSM və ya 4G vasitəsilə ötürülür.

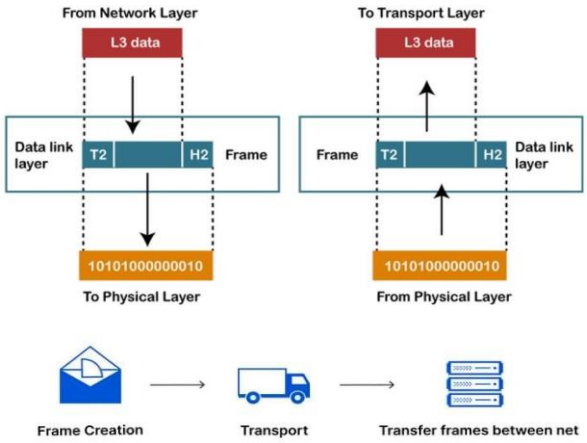


Şəkil 2.34. Fiziki səviyyə

Kanal səviyyəsində (S2) şəbəkə cihazlarının qarşılıqlı əlaqəsini təmin edən fiziki səviyyə ilə əlaqə qurulur. Məlumdur ki, iki istifadəçi yalnız iki cihazdan ibarət eyni şəbəkədə olduqda, bu ideal haldır. Bəs bu cihazlar daha çox olarsa proses necə idarə olunacaqdır? Bu suala ikinci səviyyə cavab verir. S2 informasiyanın ötürülməsi zamanı ünvanlama problemini həll edir. Bağlantı səviyyəsi bitləri qəbul edir və onları freymlərə (kadlara) çevirir. Burada əsas tapşırıq göndərənin və alıcının ünvanı ilə çərçivələr yaratmaq və sonra onları şəbəkə üzərindən ötürməkdir. Bağlantı səviyyəsinin iki alt səviyyəsi mövcuddur:

1. MAC
2. MMC

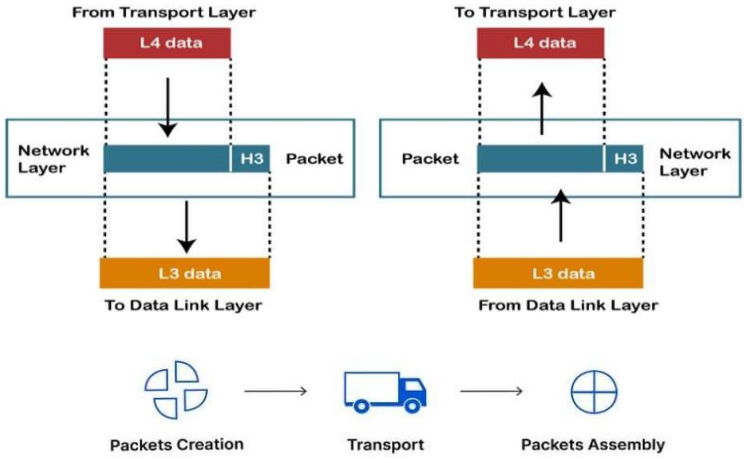
MAC (Media Girişinə Nəzarət - Media Access Control) fiziki MAC ünvanlarının təyin edilməsinə cavabdehdir. MMC (Logical Link Control) məlumatları yoxlayır, redaktə edir və ötürülməsinə nəzarət edir. Sadələşdirmək üçün biz modelin ikinci səviyyəsində MMC-ni göstəririk, lakin dəqiq desək, MMC-ni nə birinci, nə də ikinci səviyyəyə tam aid etmək olmaz. Bu hər 2 səviyyə arasındadır. Kommutatorlar S2 səviyyəsində işləyirlər, onların vəzifəsi ünvan kimi yalnız fiziki MAC ünvanlarından istifadə edərək yaradılan freymləri bir cihazdan digərinə ötürməkdir. S2 səviyyəsində ARP protokolu (Ünvan həlli protokolu-Address Resolution Protocol) aktiv şəkildə istifadə olunur. O, 64 bitlik MAC ünvanlarını 32 bitlik IP ünvanlarına və əksinə xəritələşdirir, bununla da məlumatları inkapsulyasiya və ya dekapsulyasiya edir (şəkil 2.35).



Şəkil 2.35. Kanal səviyyəsi

Şəbəkə səviyyəsində (S3) məlumat paketlərini müxtəlif şəbəkələr vasitəsilə göndərəndən alıcıya çatdırmaqdır. Şəbəkədəki hər bir cihazın unikal IP ünvanı var və bu, paketlərin müəyyən edilməsində və yönləndirilməsində əsas rol oynayır. Routerlər S2-nin SWITCH cihizaından MAC ünvanını alır və şəbəkədəki bütün potensial problemləri nəzərə alaraq bir cihazdan digərinə marşrut qurmaqla məşğul olur (şəkil 2.36).

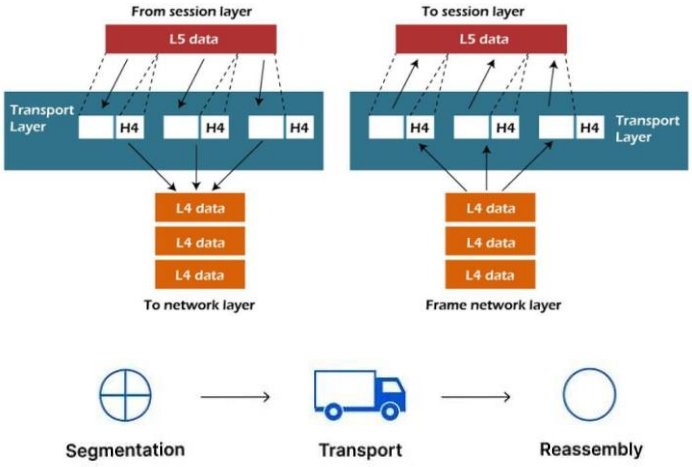
MAC ünvanları bir-birinə qoşulmuş şəbəkə kartları arasında əlaqə və ötürmə üçün istifadə edildiyi halda, IP ünvanları şəbəkələrdəki qovşaqların və hostların tanınması, yəni bir-birinə ötürülməsi prosesinə xidmət edir.



Şəkil 2.36. Şəbəkə səviyyəsi

S3 səviyyəsində də marşrutlaşdırıcı qurğuların IP və MAC ünvanlarını uyğunlaşdırmağa imkan verən ARP protokoldan istifadə olunur. Bu protokol sayəsində IP və MAC məlumatları əldə edilərək marşrutlaşdırıcının cədvəlinə daxil edilir. Bu üsulla marşrutlaşdırıcılar hansı IP ünvanlar hansı MAC ünvana uyğun olduğunu təyin edərək müvafiq qovşaqlara yönləndirir.

Nəqliyyat səviyyəsi (S4) cihazlar arasında məlumatların dəqiq çatdırılmasını təmin edir və məlumat axınına nəzarət edir. Məlumat şəbəkə üzərindən göndərildikdə, düzgün paketlərin lazımi proqramlara və cihazlara çatmasını təmin etmək vacibdir edir (şəkil 2.37).



Şəkil 2.37. Nəqliyyat səviyyəsi

S4 Host və Media səviyyələri arasında vasitəçi rolunu oynayır. Onun əsas vəzifəsi paketlərin daşınmasıdır. Təbii ki, tranzit zamanı itkilər baş verə bilər, lakin bəzi məlumat növləri digərlərindən daha çox itkiyə məruz qalır. Məsələn, mətndə saitlər itibsə, mənasını anlamaq çətinləşəcək və video axınından bir-iki kadr yoxa çıxsa, bunun son istifadəçiyə praktiki olaraq heç bir təsiri olmayacaq. Hər bir kompüterdə bir sıra portlar mövcuddur və uyğun olaraq proqram şəbəkə ilə əlaqəyə girdikdə bu xüsusi portlardan istifadə edir. Port nömrəsi hər bir proqram üçün unikaldır və unikal məlumat çatdırılma üsulunu xarakterizə edir. Beləliklə, müvafiq portdan istifadə edərək məlumat yalnız tələb olunan proqrama ötürülə bilər. Bu sistem məlumat axınını strukturlaşdırır, onun düzgün istiqamətləndirilməsini və son tətbiqlərə çatdırılmasını təmin edir. Portlar sayəsində məlumatlar təcrid olunur və istənilən proqramlara təhlükəsiz şəkildə çatdırılır, toqquşma və insidentlərin qarşısını alır. Hər bir port xüsusi məqsədə malikdir və mütəşəkkil məlumat mübadiləsini təmin edən xüsusi proqram və ya xidmətlərlə əlaqələndirilir. Bu port sistemi məlumat axınını effektiv şəkildə idarə edir, hər bir tətbiqin lazımi məlumatı müvafiq kanal vasitəsilə almasını təmin edir. Nəqliyyat səviyyəsində məlumatların mübadiləsi zamanı iki protokoldan istifadə olunur:

1. Transmissiya idarəetmə protokolu (TCP).
2. İstifadəçi datagram protokolu (UDP).

Nəqliyyat səviyyəsində itkilərə ən həssas olan məlumatların ötürülməsi zamanı çatdırılan məlumatın bütövlüyünə nəzarət edən TCP protokolundan istifadə olunur. Multimedia fayllarının ötürülməsi zamanı meydana çıxa bilən cüzi təhriflər gecikməyə səbəb olduğu üçün UDP protokolundan istifadə olunur.

TCP protokolu (Transmission Control Protocol) məlumatların etibarlı çatdırılmasını təmin edən çoxistiqamətli protokoldur. Məlumat paketlərini göndərməzdən əvvəl TCP məlumat qəbul edən tərəfə hazır olması barədə sorğu göndərərək qəbuledicilə əlaqəyə girir və sorğu təsdiq olunduqdan sonra məlumatın etibarlı şəkildə göndərilməsi prosesi uğurla həyata keçirilir. Üçtərəfli əl sıxma kimi tanınan bu proses məlumatların düzgün və ardıcıl şəkildə çatdırılmasını təmin edir. Məsələn, serverlə əlaqə yaratmaq üçün SYN (sinxronizasiya) paketi göndərilir, bu paket SYN-ACK təsdiqləmə paketi ilə cavab verir və sonra ACK əl sıxması baş verir. Bu, məlumat mübadiləsi göndərən və alıcı arasında təhlükəsiz əlaqə yaradır. TCP həmçinin məlumatın bütövlüyünü təmin etmək üçün itirilmiş məlumat və ya zədələnmiş paketlər kimi səhvləri aşkar etmək və düzəltmək mexanizmlərini ehtiva edir. Bu, xüsusilə e-poçt, veb-saytlar və fayl endirmələri kimi missiya baxımından kritik

proqramlarda etibarlı və müntəzəm məlumat ötürülməsini təmin edir. TCP-nin istifadəsi məlumat mübadiləsində yüksək etibarlılığın təmin edilməsi, itkisiz və təhrif edilmədən tam məlumatın alınmasını nəzərdə tutur. Beləliklə, TCP dəqiq və təhlükəsiz məlumat ötürülməsi tələb olunduğu, hər bir məlumat bitinin vacib olduğu hallarda geniş istifadə olunur.

UDP (User Datagram Protocol) protokolu məlumatların ötürülməsinə nəzarət mexanizmlərinin olmaması ilə TCP-dən fərqlənir. TCP-dən fərqli olaraq, UDP etibarlı əlaqə yaratmır və məlumatı göndərməzdən əvvəl qəbul edən qovşağın təsdiqini yoxlayır. O, əlaqə yaratmadan və bütün paketlərin gəlməsinə zəmanət vermədən məlumat paketlərini ardıcıl olaraq göndərir. Bu, məlumatın daha tez çatdırılmasına imkan verir, lakin ötürülən məlumatların tamlığına və ya düzgünlüyünə zəmanət vermir. Buna görə də UDP informasiyanın ötürülmə sürətinin onun tamlığından və ya dəqiqliyindən daha vacib olduğu vəziyyətlərdə geniş istifadə olunur. Belə sahələrə misal olaraq audio və video axını xidmətlərini göstərmək olar ki, burada ötürülmənin çevikliyi böyük əhəmiyyət kəsb edir. Video və audio mübadilə proqramlarında UDP çatdırılma nəzarət mexanizminin olmaması səbəbindən müvəqqəti sistemdə müəyyən fasilələr və ya paket itkisi yarana bilər. Bununla belə, sürətlilik xüsusiyyətinə görə UDP məlumat ötürülməsi mühitlərində prioritet seçim olaraq qalır. Bir sözlə, TCP etibarlı məlumat ötürülməsini təmin etdiyi halda, UDP məlumat bütövlüyü baxımından sürətli, lakin daha az etibarlı ötürülmə təmin edir. TCP və UDP protokolunun fərqləndirici cəhətləri cədvəl 2.2-də təsvir olunmuşdur.

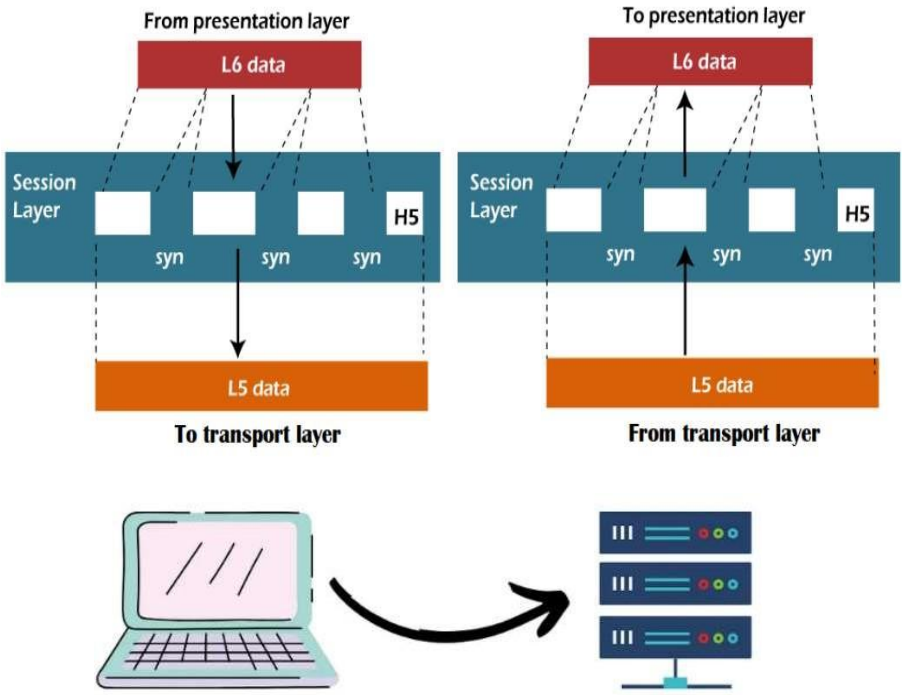
Cədvəl 2.2.

TCP və UDP protokolun fərqləndici cəhətləri

TCP protokolu	UDP protokolu
Məlumatları ardıcıl olaraq ötürür	Məlumatları təsadüfi qaydada ötürür
Səhvləri izləyir	Məlumatı yoxlamadan göndərir
Yavaş işləyir	Sürətli işləyir
Mətn və fotoşəkillər üçün istifadə olunur	Video və audio üçün istifadə olunur

Seans səviyyəsi (S5) OSI modelindəki sessiya səviyyəsi şəbəkədəki cihazlar arasında rabitə seanslarının idarə edilməsi və qurulması üçün

cavabdehdir. Bu səviyyə rabitə seanslarını başlatmaq, idarə etmək və dayandırmaq imkanını verir (şəkil 2.38).

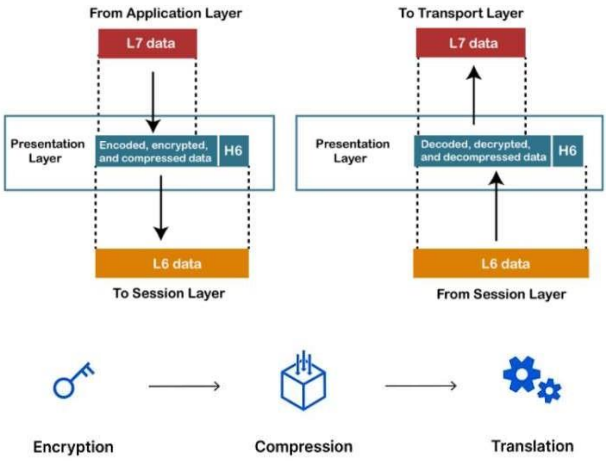


Şəkil 2.38. Seans səviyyəsi

S5 emal olunmuş məlumatlarla işləyir. Bununla yanaşı emal olunmuş məlumatlar həmçinin S6 və S7 səviyyələrində də istifadə olunur. Seans səviyyəsinin iş mexanizmi aşağıdakı kimidir: o, proqramlar arasında qarşılıqlı əlaqəni idarə edir, tapşırıqları sinxronlaşdırır, sessiyanı başa çatdırır və məlumat mübadiləsi rejimlərini aktivləşdirir. Beləliklə, S5 uzaqdan idarəetmə (remote controller) prosesini formalaşdırır. Bu səviyyəni bir nümunə üzərindən izahını aparaq. Şəbəkə üzərindən video zəng S5 səviyyəsi ilə reallaşdırılır. Video zəng zamanı iki məlumat axınının (audio və video) sinxron şəkildə təşkili tələb olunur. İki nəfərin söhbətinə üçüncü şəxs əlavə olunduqda o, artıq konfrans xidmətinə çevrilir. Beşinci səviyyənin əsas vəzifəsi həmsöhbətlərin bir-birini başa düşməsinə şərait yaratmaqdır.

Təqdimat səviyyəsi (S6) verilənlərin təqdim edilməsinə, onların müxtəlif qurğular və əməliyyat sistemləri arasında uyğunluğunun və şərhinin təmin edilməsinə cavabdehdir. Bu səviyyə şəbəkə üzərindən səmərəli ötürmə üçün

məlumatların kodlaşdırılmasını, sıxılmasını və şifrələnməsini təmin edir (şəkil 2.39).



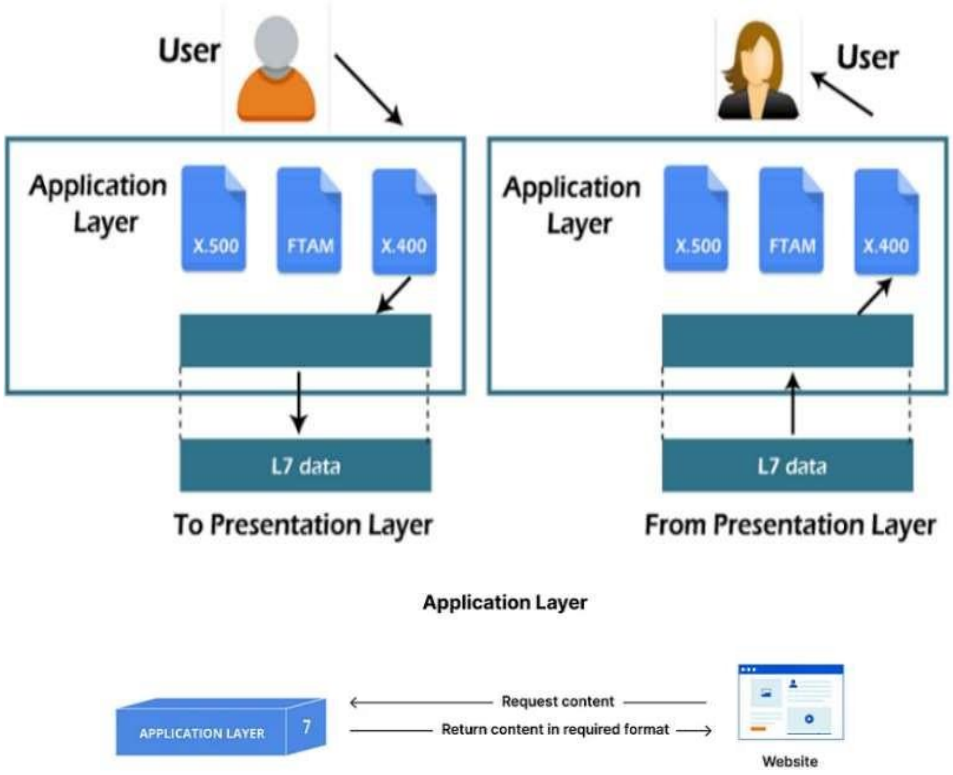
Şəkil 2.39. Təqdimat səviyyəsi

S6 həmçinin məlumatların qəbuledicinin başa düşə biləcəyi formatlara çevrilməsinə və zəruri hallarda yenidən geri qaytarılmasına xidmət edir. S6 müxtəlif sistemlər arasında məlumat mübadiləsi üçün məlumat formatlarının standartlaşdırılmasını və uyğunlaşdırılmasını təmin edir. Bu səviyyədə ötürülmə zamanı məlumat zədələnərsə onun bərpası funksiyaları, həmçinin şifrələmə və autentifikasiya vasitəsilə məlumatların təhlükəsizliyi təmin edilir. Qeyd olunanlarla yanaşı S6 həm də şəkillərin (JPEG, GIF və s.), eləcə də video və audionun (MPEG, QuickTime formatında) təqdimatı ilə də məşğul olur (cədvəl 2.1).

Tətbiq səviyyəsi (S7) istifadəçilərə şəbəkə ilə qarşılıqlı əlaqə yaratmağa imkan verən tətbiq proqramları üçün interfeys təqdim edir. Buraya HTTP (veb serverlər üçün), FTP (faylların ötürülməsi üçün) və SMTP (e-poçt üçün) kimi müxtəlif proqram protokolları daxildir (şəkil 2.40).

OSI modelinin tətbiqi səviyyəsində istifadəçinin şəbəkə ilə birbaşa əlaqəsi baş verir. Bu səviyyə veb brauzerlər, e-poçt, fayl serverləri və digər proqramlar kimi şəbəkə xidmətləri və resurslarına çıxışı təmin edir. O, şəbəkə xidmətləri ilə işləmək və məlumat ötürmələrini idarə etmək üçün interfeys təqdim edir. Tətbiq səviyyəsində istifadəçilər müxtəlif tapşırıqları yerinə yetirə bilərlər, o cümlədən mesajlaşma, faylları yükləmək, internetə baxmaq və s. Burada

məlumatların son işlənməsi, onun istifadəçi dostu (UX/UI dizaynı) formatına çevrilməsi baş verir.



Şəkil 2.40. Tətbiq səviyyəsi

Tətbiq səviyyəsinə istifadəçilərə şəbəkə ilə qarşılıqlı əlaqədə olmaq və onun resurslarından istifadə etmək imkanı verən müxtəlif protokollar və proqramlar daxildir. O, şəbəkəyə yüksək səviyyəli çıxışı təmin edir, onun işinin təfərrüatlarını istifadəçidən gizlədir. Bu səviyyədə işləyən proqramlar məlumat mübadiləsi və şəbəkə resurslarını idarə etmək üçün müxtəlif şəbəkə protokollarından istifadə edir. Tətbiq səviyyəsi onlayn istifadəçi təcrübəsinin açarıdır, çünki istifadəçilər müxtəlif xidmətlər və tətbiqlərlə qarşılıqlı əlaqədə olurlar. O, şəbəkə resurslarının istifadəsində rahatlıq və səmərəliliyi təmin edərək, onları son istifadəçilər üçün əlçatan və başa düşülən edir.

TCP/IP modeli[17]. TCP/IP OSI modelindən daha qədimdir və 1970-ci illərdə ARPANET-də ABŞ Müdafiə Nazirliyi tərəfindən yaradılmışdır. TCP/IP

[17] https://www.javatpoint.com

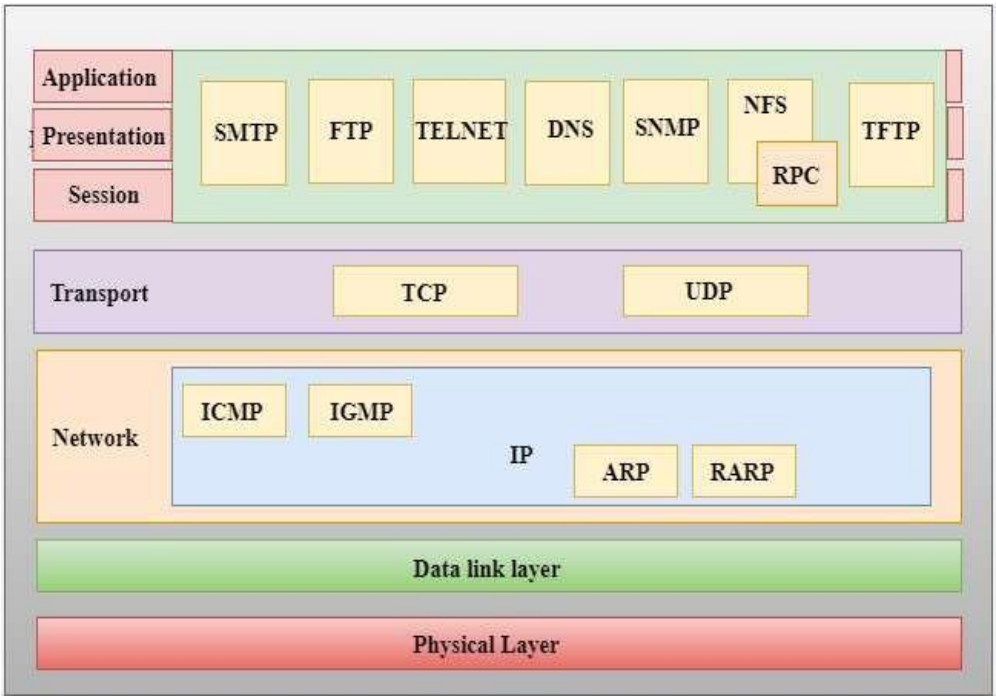
modeli məlumatların şəbəkə üzərindən necə ötürüldüyünü müəyyən edən 5 səviyyədən ibarətdir (cədvəl 2.3).

Cədvəl 2.3.

TCP/IP modeli səviyyələri

	TCP/IP modeli	PDU	Xüsusiyyətlər		
5	Tətbiq səviyyəsi	Verilənlər			
4	Nəqliyyat səviyyəsi	Seqment Dataqram		Dekapsulyasiya (S1-S7) ↑	İnkapsulyasiya (S7-S1) ↓
3	Şəbəkə səviyyəsi	Paket	MEDİA		
2	Kanal səviyyəsi	Kadr			
1	Fiziki səviyyə	Bit			

TCP/IP modelinin səviyyələri OSI modelinin səviyyələri ilə analojidir. TCP/IP modelində səviyyələr üzrə istifadə olunan protokollar şəkil 2.41-də təsvir olunmuşdur.



Şəkil 2.41. TCP/IP modelində səviyyələr üzrə istifadə olunan protokolların təsviri

OSI və TCP/İP modeli fərqli xüsusiyyətləri cədvəl 2.4-də göstərilmişdir.

Cədvəl 2.4.

OSI və TCP/İP modeli fərqli xüsusiyyətləri

OSI Modeli	TCP/IP Modeli
Açıq Sistem Qarşılıqlı Əlaqə deməkdir.	Bu Transmission Control Protocol deməkdir.
OSI modeli ISO (Beynəlxalq Standartlar Təşkilatı) tərəfindən hazırlanmışdır.	O, ARPANET (Advanced Research Project Agency Network) tərəfindən hazırlanmışdır.
Şəbəkə və son istifadəçi arasında rabitə şlüzü kimi istifadə edilən müstəqil standart və ümumi protokoldur.	İnternetin inkişafına səbəb olan standart protokollardan ibarətdir. Bu, hostlar arasında əlaqəni təmin edən bir rabitə protokoludur.
OSI modelində nəqliyyat səviyyəsi paketlərin çatdırılmasına zəmanət verir.	Nəqliyyat səviyyəsi paketlərin çatdırılması üçün zəmanət vermir. Ancaq yenə də etibarlı bir model olduğunu söyləyə bilərik.
Bu model şaquli yanaşmaya əsaslanır.	Bu model üfüqi bir yanaşmaya əsaslanır.
Bu modeldə seans və təqdimat səviyyələri fərqlidir.	Bu modeldə sessiya və təqdimat səviyyəsi fərqli səviyyələr deyil. Hər iki səviyyə tətbiq səviyyəsinə daxildir.
O, həmçinin müxtəlif şəbəkələrin qurulduğu bir istinad modeli kimi tanınır. Məsələn, TCP/IP modeli OSI modelindən əvvəl qurulmuşdur. O, həm də bələdçilik vasitəsi kimi istinad edilir.	OSI modelinə uyğunlaşdırılmış modeldir.

OSI modelindəki protokollar gizlidir və texnologiya dəyişdikdə asanlıqla dəyişdirilə bilər.	Bu modeldə protokol asanlıqla dəyişdirilə bilməz.
7 səviyyədən ibarətdir.	5 səviyyədən ibarətdir.
OSI modeli xidmətləri, protokolları və interfeysləri müəyyən edir, həmçinin onlar arasında düzgün fərqi təmin edir. Protokoldan asılı deyildir.	TCP/IP modelində xidmətlər, protokollar və interfeyslər düzgün ayrılmayıb. Protokoldan asılıdır.
Bu modelin istifadə dairəsi geniş deyildir.	Bu model çox istifadə olunur.
Router, anakart, açarlar və digər aparat cihazları kimi cihazlara standartlaşdırma təmin edir.	Cihazlara standartlaşdırma təmin etmir. Müxtəlif kompüterlər arasında əlaqə təmin edir.

OSI modelinin əsas prinsipləri. OSI şəbəkə modelinin dizayn prinsipi verilənlərin ötürülməsi prosesini bir neçə abstraksiya səviyyəsinə bölən iyerarxik yanaşmaya əsaslanır. Bu səviyyələr məlumatların şəbəkə üzərindən göndəricidən qəbulediciyə ötürülməsi üçün tələb olunan funksiyalar ardıcıllığıdır. Məlumatların ötürülməsi prosesi həmişə göndərən cihazı, qəbuledici cihazı, həmçinin ötürülməli və qəbul edilməli olan məlumatları əhatə edir. Sadə istifadəçi nöqteyi-nəzərindən tapşırıq elementardır - bu məlumatları götürüb göndərməlisiniz. Məlumatların göndərilməsi və qəbulu zamanı baş verən hər bir proses yeddi qatlı OSI modeli tərəfindən ətraflı təsvir edilmişdir. Yeddinci səviyyədə məlumat verilənlər şəklində, birinci səviyyədə isə bit (0 və 1) şəklində təmsil olunur. Məlumatın göndərildiyi və verilənlərdən bitlərə keçdiyi prosesə inkapsulyasiya deyilir. Birinci səviyyədə bitlərdə alınan məlumat yeddinci səviyyədə verilənlərə daxil olduqda əks proses dekapsulyasiya adlanır. Yeddi səviyyənin hər birində məlumat PDU (Protocol Data Unit) protokolu ilə təqdim olunur. Bir misala baxaq. İstifadəçi 1 məlumat şəklində yeddinci səviyyədə işlənən şəkil göndərir, verilənlər bütün səviyyələrdən keçərək ən aşağıya (birinci) keçməlidir, burada bit kimi təqdim

olunacaq. Bu proses inkapsulyasiya adlanır. İstifadəçi 2-nin kompüteri yenidən verilənlərə çevrilməli olan bitləri alır. Bu tərs proses dekapsulyasiya adlanır.

PORT NÖMRƏLƏRİ VƏ ŞƏBƏKƏ PROTOKOLLARI

Port nömrələri və şəbəkə protokolları kompüter şəbəkələrində trafikə nəzarət edən və yönləndirən şəbəkə arxitekturasının mühüm hissəsi olmaqla xüsusi xidmətləri və proqramları müəyyən etmək üçün istifadə olunur. Şəbəkədən istifadə edən hər bir proqram və ya xidmət adətən müəyyən bir porta bağlıdır və xüsusi şəbəkə protokolu ilə işləyir. Port nömrəsi əməliyyat sisteminə daxil olan şəbəkə trafikini düzgün tətbiq və ya xidmətə yönləndirməyə kömək edən rəqəmli identifikatordur. Kompüter məlumatı şəbəkə üzərindən göndərən zaman o, məlumat paketinin başlığına mənbə port nömrəsini və təyinat port nömrəsini daxil edir. Bu, marşrutlaşdırıcılara və digər şəbəkə cihazlarına verilənlərin hansı proqrama və ya xidmətə yönləndirilməli olduğunu müəyyən etməyə imkan verir. Məlumat qəbul edərkən, cihaz əməliyyat sistemi səviyyəsində məlumatları düzgün proqrama çatdırmaq üçün port nömrəsindən istifadə edir.

Port nömrələrinin təsnifatı[18]. Port nömrələri məqsədlərinə və xidmət etdikləri xüsusi protokollara və ya xidmətlərə görə aşağıdakı kimi təsnif edilir.

Qeydiyyatdan keçmiş portlar.

Tanınmış portlar.

Xüsusi portlar.

Qeydiyyatdan keçmiş portlar 1024 – 49151 aralığında təyin olunur. Bu portların əsas məqsədi İnternetdən Təyin edilmiş Nömrələr Təşkilatı (IANA) tərəfindən sistem səviyyəsində və ya tanınmış olmayan xüsusi proqramlar və

[18] Port Checker - Check Open Ports Online (dnschecker.org)
https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play
Metasploit: http://www.metasploit.com/ also a cheat sheet for Metasploit
http://www.openvas.org/
http://lifehacker.com/198946/how-to-portscan-your-computer-for-security-holes
http://www.techradar.com/us/news/networking/how-to-secure-your-tcp-ip-ports-633089
http://www.techrepublic.com/article/lock-it-down-develop-a-strategy-for-securing-ports-on-your-servers/
https://www.grc.com/default.htm
https://www.avg.com/en/signal/prevent-router-hacking
http://security.stackexchange.com/questions/77112/danger-of-default-router-password
http://www.acunetix.com/blog/web-security-zone/the-email-that-hacks-you/

xidmətlər tərəfindən istifadə üçün qeydiyyata alınıb. Məsələn, Port 3306 ən məşhur verilənlər bazası idarəetmə sistemlərindən (DBMS) biri olan MySQL protokolu üçün qeydiyyatdan keçmişdir. MySQL müxtəlif veb proqramlarda, CMS (məzmun idarəetmə sistemləri), e-ticarət və digər növ proqramlarda strukturlaşdırılmış məlumatları saxlamaq və idarə etmək üçün istifadə olunur. Port 3306 adətən müştərilər və MySQL serverləri arasında ünsiyyət üçün istifadə olunur.

Tanınmış portlar 0 – 1023 aralığında təyin olunur. Bu portlar ən çox istifadə olunan xidmətlər və protokollar üçün IANA tərəfindən qorunur. Məsələn, 80 port HTTP üçün, port 25 SMTP üçün istifadə olunur (Simple Mail Transfer Protocol).

Xüsusi portlar 49152 – 65535 aralığında təyin olunur. Bu portlar lokal testlər, müvəqqəti bağlantılar və digər ictimai olmayan məqsədlər üçün istifadə olunur. Onlar IANA tərəfindən qeydiyyata alınmayıb və istənilən lokal və ya xüsusi şəbəkə ehtiyacları üçün istifadə oluna bilər. Bu təsnifat şəbəkə resurslarından strukturlaşdırılmış və səmərəli istifadəni təmin edərək port nömrələrini təşkil etməyə və idarə etməyə kömək edir.

TCP/IP səviyyəsi tərəfindən təşkil edilən ən ümumi protokollar aşağıdakı Cədvəl 2.5-də təqdim olunur. TCP/IP modelinin Tətbiq səviyyəsində verilənlərin ötürülməsini təmin etmək və müxtəlif şəbəkə funksiyalarını yerinə yetirmək üçün müxtəlif protokollardan istifadə olunur.

Cədvəl 2.5.

TCP/IP modeli və onların protokolları

TCP/IP səviyyələri	**Protokol**
Tətbiq	HTTP HTTPS/TLS SMTP POP3 IMAP FTP DNS DHCP SNMP SSH

Nəqliyyat	NTP TCP UDP
İnternet	IPv4 IPv6 ICMP IGMP
Şəbəkə	ARP

Tətbiq səviyyəsində ən çox yayılmış protokollar cədvəldən göründüyü kimi aşağadakılardır:

1. HTTP (HyperText Transfer Protocol) - İnternetdə veb səhifələri və digər hipermətn sənədlərini ötürmək üçün istifadə olunur. Məsələn, brauzerdə veb səhifəni açarkən.

2. HTTPS (HyperText Transfer Protocol Secure) - təhlükəsiz məlumat ötürülməsini təmin etmək üçün şifrələmədən istifadə edən HTTP-nin təhlükəsiz versiyasıdır. Tez-tez bank kartı məlumatları kimi məxfi məlumatları ötürərkən istifadə olunur.

SMTP (Simple Mail Transfer Protocol) - E-poçt serverləri və müştərilər arasında e-poçt göndərmək və çatdırmaq üçün istifadə olunur.

POP3 (Post Office Protocol version 3) - E-poçtu poçt serverindən müştəri kompüterinə yükləmək üçün istifadə olunur.

IMAP (Internet Message Access Protocol)- Müştəri cihazlarına poçt serverində saxlanılan e-poçtlara daxil olmaq və idarə etmək imkanı verir.

FTP (Fayl Transfer Protokolu)-Şəbəkədəki kompüterlər arasında faylları ötürmək üçün istifadə olunur. İstifadəçilər faylları uzaq serverlərə yükləyə və yükləyə bilərlər.

DNS (Domain Name System)- Domen adlarını (məsələn, www.example.com) IP ünvanlarına və əksinə həll etmək üçün istifadə olunur.

DHCP (Dinamik Host Konfiqurasiya Protokolu)- Kompüterlər və şəbəkədəki digər cihazlar üçün şəbəkə parametrlərinin (məsələn, IP ünvanları) avtomatik konfiqurasiyasını təmin edir.

SNMP (Sadə Şəbəkə İdarəetmə Protokolu)- Şəbəkə cihazlarını uzaqdan idarə etməyə, onların vəziyyətinə nəzarət etməyə və statistika toplamağa imkan verir.

SSH (Təhlükəsiz Qabıq)- Şifrələnmiş əlaqə üzərindən kompüterlərə təhlükəsiz uzaqdan qoşulma və nəzarəti təmin edir.

NTP (Network Time Protocol) - şəbəkədəki kompüterlər arasında vaxtı sinxronlaşdırmaq üçün istifadə edilən protokoldur. O, cihazlarda dəqiq vaxtı və paylanmış şəbəkə üzrə vaxt ardıcıllığını təmin edir.

Bu protokollar TCP/IP proqram təminatı səviyyəsində müxtəlif şəbəkə funksiyaları və proqramları təmin edir.

Nəqliyyat səviyyəsinin protokolları şəbəkədəki qovşaqlar arasında məlumatların etibarlı çatdırılmasını təmin edir. Onlar İnternet səviyyəsinin protokolları üzərində işləyir və son cihazlar arasında məlumat ötürülməsini təmin edir. Ən çox yayılmış nəqliyyat səviyyəsi protokollarına TCP və UDP daxildir.

Transmissiya İdarəetmə Protokolu (TCP) - Verilənlərin düzgün qaydada çatdırılmasını təmin edən və onları yenidən ötürmək üçün itirilmiş paketləri aşkarlayan etibarlı məlumat çatdırılması protokoludur. Veb saytlar, e-poçt, fayl köçürmələri və s. kimi etibarlı məlumat ötürülməsinin zəruri olduğu tətbiqlərdə istifadə olunur.

İstifadəçi Datagram Protokolu (UDP) - Düzgün qaydada çatdırılmaya zəmanət verməyən və itirilmiş paketləri aşkar etməyən sadə və etibarsız məlumat çatdırılması protokoludur. Aşağı gecikmənin etibarlı məlumat ötürülməsindən daha vacib olduğu proqramlarda, məsələn, video axını, onlayn oyunlar, yayımlar və s.

Bu iki protokol - TCP və UDP nəqliyyat səviyyəsində əsas olanlardır və şəbəkədə əlaqəni təmin etmək üçün geniş istifadə olunur. Onlar müəyyən bir tətbiqin tələblərindən asılı olaraq müvafiq protokolu seçməyə imkan verən müxtəlif məlumat ötürmə xüsusiyyətlərini təmin edir.

İnternet səviyyəsi protokolları şəbəkədəki cihazlar arasında məlumat paketlərinin marşrutlaşdırılmasını və çatdırılmasını təmin edir. Bu təbəqədə ən çox yayılmış protokollar aşağıdakılardır:

1. IPv4 (İnternet Protokolunun 4-cü versiyası)- IPv4 İnternetdə əsas marşrutlaşdırma və məlumatların çatdırılması protokoludur. O, 32 bitlik ünvanlardan istifadə edir və məlumat paketlərinin identifikasiyası və marşrutlaşdırılmasını təmin edir.

2. IPv6 (İnternet Protokolunun 6-cı versiyası)- IPv6 IPv4-ün məhdudiyyətlərini, o cümlədən ünvan məkanının tükənməsini həll etmək üçün yaradılmış IP protokolunun növbəti nəslidir. IPv6 128-bit ünvanlardan istifadə edir ki, bu da böyük bir ünvan sahəsi təmin edir və təkmilləşdirilmiş təhlükəsizlik mexanizmlərini və multicast rabitə dəstəyini ehtiva edir.

3. ICMP (Internet Control Message Protocol). ICMP səhv mesajları göndərmək, şəbəkə vəziyyətini izləmək və diaqnostika aparmaq üçün istifadə olunur. Məsələn, ICMP paketlər çatdırılmadıqda səhv mesajları göndərmək və ping əmrindən istifadə edərək hostların mövcudluğunu yoxlamaq üçün istifadə olunur.

IGMP (İnternet Qrup İdarəetmə Protokolu). IGMP IP şəbəkələrində multicast rabitəsini idarə etmək üçün istifadə olunur. O, hostlara və marşrutlaşdırıcılara hansı hostların multicast qruplarının üzvləri olduğunu müəyyən etməyə və şəbəkə üzrə multicast paketlərinin yayımı prosesinə nəzarət etməyə imkan verir.

Şəbəkə səviyyəsinin ən geniş protokolu ARP (Address Resolution Protocol) hesab olunur. Lokal şəbəkədəki şəbəkə cihazları arasında əlaqə yaratmaq üçün istifadə olunan şəbəkə səviyyəsi protokoludur. Onun əsas işi cihazın IP ünvanını onun fiziki MAC ünvanı ilə əlaqələndirməkdir. ARP 2 sorğu və cavab rejimində işləyir.

ARP Sorğusu - Bir cihaz yerli şəbəkədəki başqa bir cihaza məlumat paketi göndərməli olduqda və yalnız onun IP ünvanı məlum olduqda, yayım ünvanına ARP sorğusu göndərir. Bu sorğuda cihaz soruşur: "X.X.X.X IP ünvanı kimdədir?" Sorğu qoşulmaq istədiyiniz cihazın IP ünvanını müəyyən edir.

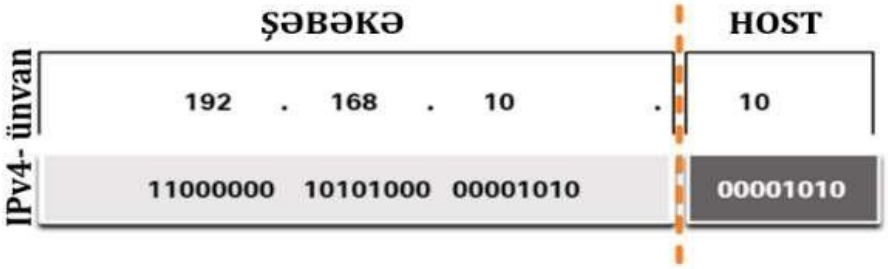
ARP cavabı - Göstərilən IP ünvanı olan cihaz ARP sorğusunu aldıqdan sonra ona ARP cavabı göndərməklə cavab verir. Bu cavab onun öz IP ünvanını və ona uyğun MAC ünvanını müəyyən edir. Bu yolla, sorğu edən cihaz hədəf cihaza uğurla çatdırılacaq məlumat çərçivəsi yaratmaq üçün lazımi məlumatları alır.

ARP Ethernet LAN-larda IP ünvanlarına əsasən cihazların fiziki ünvanlarını təyin etmək üçün geniş istifadə olunur. Bu, müxtəlif ünvan boşluqlarından (IP və MAC) istifadə etmələrinə baxmayaraq, cihazların yerli şəbəkədə bir-biri ilə effektiv əlaqə saxlamasına imkan verir.

İNTERNET SƏVİYYƏSİNİN PROTOKOLLARI: IPv4 və IPv6

IPv4 ünvanı (İnternet Protokolunun 4-cü versiyası)[19] internetdə cihazı müəyyən etmək üçün istifadə olunan unikal rəqəmsal identifikatordur. IPv4 ünvanı 32 bitdən ibarətdir (adətən dörd oktet şəklində təmsil olunur) və nöqtəli onluq formatda yazılır. Məsələn, 192.168.1.1. Hər bir oktet 0-dan 255-ə qədər qiymətə malik ola bilər. IPv4 ünvanlanması sinif prinsiplərindən istifadə edir, lakin ən çox yayılanlar kiçik ev və ofis şəbəkələri üçün istifadə olunan C sinif ünvanlarıdır. IPv4-ün məhdud sayda ünvanları var (təxminən 4,3 milyard) və bu, 128 bitdən istifadə edən və əla ünvan genişlənməsini təmin edən yeni IPv6 standartının yaradılmasına gətirib çıxardı. IPv4 ünvanın strukturu iki hissədən ibarətdir: şəbəkə hissəsi və host hissəsi (şəkil 2.42).

Şəkildə IPv4 ünvanı 192.168.10.10 göstərilmişdir. Bu onluq ünvan kodu 11000000 10101000 00001010 00001010 ikilik koda çevrilmişdir. IP ünvanda şəbəkə hissəsini 192.168.10. kod, host hissəsini kod.kod.kod.10 təsvir edir.



Şəkil 2.42. IPv4-ünvan strukturu

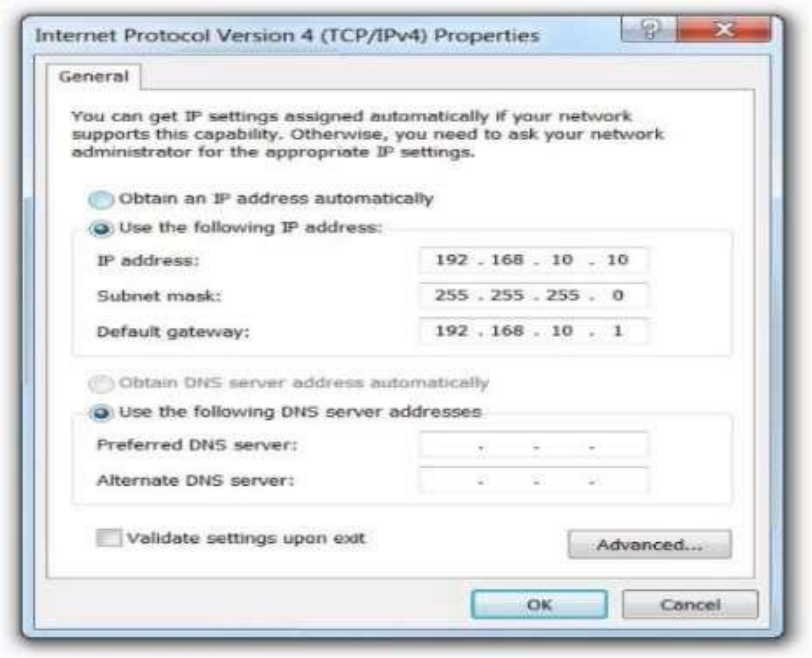
Şəbəkə hissəsi cihazın aid olduğu şəbəkəni müəyyən edir. Dəyişən uzunluqlu alt şəbəkə (VLSM) istifadə edilərsə, şəbəkə hissəsinin ölçüsü ünvan sinfindən və ya alt şəbəkə maskasından asılıdır.

Host hissəsi şəbəkə daxilində xüsusi cihazı müəyyən edir. Host hissəsinin ölçüsü şəbəkə hissəsindən sonra qalan ünvanın uzunluğu ilə müəyyən edilir. Şəbəkə və host hissələrinə bölünmə marşrutlaşdırıcılara paketləri şəbəkə üzrə səmərəli şəkildə nəql etməyə imkan verir, paketi xüsusi cihaza çatdırmaq üçün

[19] Зима В.М. Безопасность глобальных сетевых технологий / В.М.Зима, А.А.Молдовян, Н.А.Молдовян. СПб.; БХВ-Петербург, 2019. – 320 с
Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина М.: Национальный Открытый Университет «ИНТУИТ», 2014. 378 с.
Олифер В.Г. Безопасность компьютерных сетей. М.: Горячая линия - Телеком, 2018. 644с.

marşrutu və host hissəsindən məlumatı müəyyən etmək üçün şəbəkə hissəsindən məlumatlardan istifadə edir.

Alt şəbəkə maskası. Alt şəbəkə maskası, IP ünvanının hansı hissəsinin şəbəkəyə, hansı hissəsinin isə qovşağına (host) aid olduğunu müəyyən edən bitlər ardıcıllığıdır. Şəbəkə hissəsini göstərən birlərdən və host hissəsini göstərən sıfırlardan ibarətdir. Məsələn, 192.168.1.1 IP ünvanımız və 255.255.255.0 alt şəbəkə maskamız varsa, ünvanın ilk 24 biti (ilk üç oktet) şəbəkəyə xasdır, sonuncu oktet isə hostlar üçün qorunur (şəkil 2.43).



Şəkil 2.43. IPv4 konfiqurasiyası

Alt şəbəkə maskası adətən IP ünvanı ilə birlikdə yazılır, məsələn, "192.168.1.1/24", burada "/24" alt şəbəkə maskasındakı bitlərin sayını göstərir. Alt şəbəkə maskasından istifadə edərək, şəbəkədəki qurğular IP ünvanının yerli şəbəkəyə aid olub-olmadığını və ya ünvanın digər şəbəkələrə yönləndirmə üçün təyin edilib-edilmədiyini müəyyən edə bilər.

Prefiks uzunluğu. CIDR (Classless Inter-Domain Routing) notasiyası kimi də tanınır, alt şəbəkə maskasını təyin etməyin sadələşdirilmiş üsuludur. Maskanı dörd nöqtəli oktet kimi yazmaq əvəzinə, biz IP ünvanının şəbəkə hissəsini təmsil edən bitlərin sayını təyin edir. Prefiksin uzunluğunu xarakterizə edən cədvəl 2.6-də təsvir olunmuşdur.

Cədvəl 2.6.

Alt şəbəkə maskası və prefiks uzunluğunu

Alt maska	32 bitlik ünvan	Prefiksin uzunluğu
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Şəbəkənin təyini üzrə VƏ (AND) məntiq əməliyyatı. Məntiqi AND əməliyyatı diskret məntiqdə istifadə olunan üç əsas ikili əməliyyatdan biridir. Digər iki operator OR və NOT-dur. AND əməliyyatı şəbəkə ünvanını təyin etmək üçün istifadə olunur. Məntiqi VƏ (AND) iki bitin müqayisəsidir, nəticələri aşağıdakı şəkildə göstərilmişdir.

1 AND 1 = 1

0 AND 1 = 0

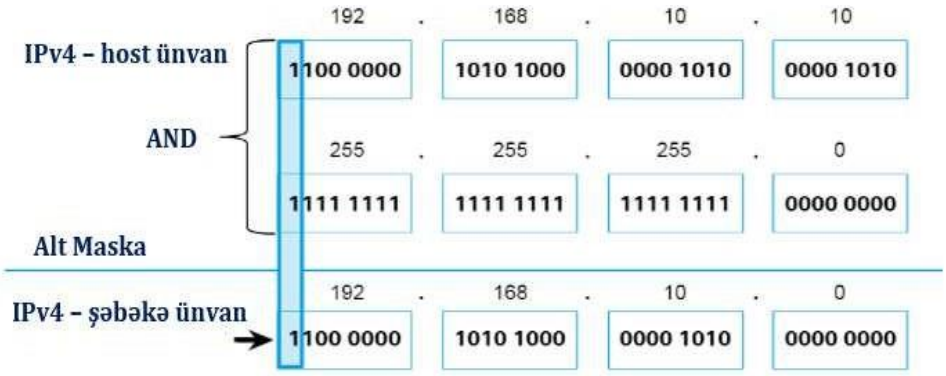
1 AND 0 = 0

0 AND 0 = 0

Qeyd: Rəqəmsal məntiqdə 1 Doğru, 0 isə Yanlış deməkdir. AND əməliyyatından istifadə edərkən nəticənin True (1) olması üçün hər iki giriş dəyəri True (1) olmalıdır. IPv4 qovşağının şəbəkə ünvanını müəyyən etmək üçün məntiqi AND IPv4 ünvanına və alt şəbəkə maskasına bit-bit tətbiq edilir (şəkil 2.44).

Şəbəkə ünvanını təyin etmək üçün AND əməliyyatından necə istifadə olunacağını nümayiş etdirmək üçün şəkildə göstərildiyi kimi IPv4 ünvanı 192.168.10.10 və alt şəbəkə maskası 255.255.255.0 olan hostu nəzərdən keçirilir. IPv4 host ünvanı (192.168.10.10) - nöqtəli onluq və ikili formatda hostun IPv4 ünvanı. Subnet Mask (255.255.255.0) - Nöqtəli onluq və ikili formatda hostun alt şəbəkə maskası. Şəbəkə Ünvanı (192.168.10.0) - IPv4

ünvanı və alt şəbəkə maskası arasında məntiqi VƏ əməliyyat IPv4 şəbəkə ünvanının nöqtəli onluq və ikili notasiyada göstərilməsi ilə nəticələnir.

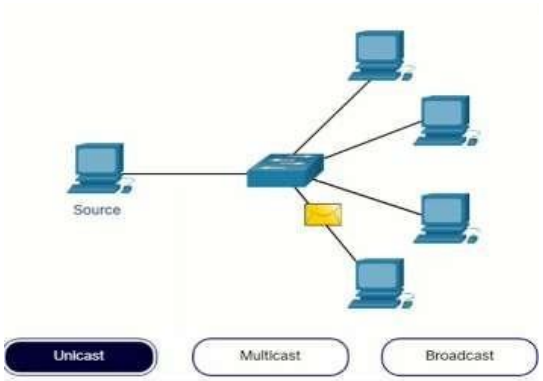


Şəkil 2.44. AND əməliyyatının tətbiqi

IPv4 ünvanlamanın növləri. Hər şəbəkədə üç növ IP ünvanı mövcuddur:

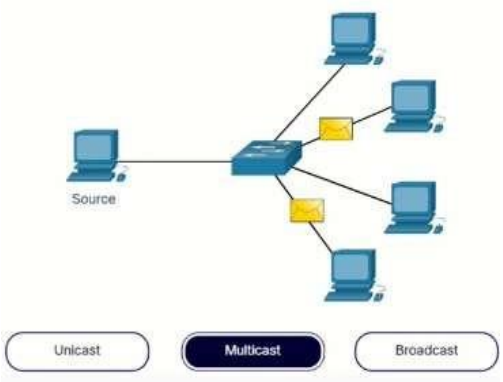
1. Unicast şəbəkə ünvanı.
2. Multicast şəbəkə ünvanı.
3. Broadcast şəbəkə ünvanı.

Unicast ünvan şəbəkənin özünü müəyyən edən ünvandır. Şəbəkə ünvanında host hissəsinin bütün bitləri 0-a təyin edilir. Məsələn, 192.168.1.0/24 ünvanlı şəbəkəmiz varsa, bu şəbəkənin şəbəkə ünvanı 192.168.1.0 olacaqdır. Unicast ünvanlar adi şəbəkələrdə və İnternetdə ən çox yayılmış ünvanlardır. Onlar bir cihazı müəyyənləşdirirlər və trafik unikal maşın üçün nəzərdə tutulub (şəkil 2.45).



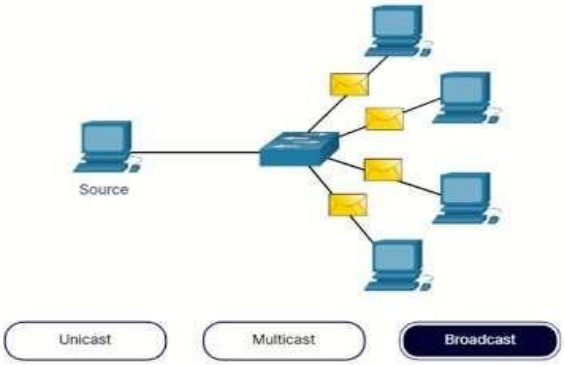
Şəkil 2.45. Unicast ünvanlama rejimi

Host ünvanı şəbəkədə müəyyən bir cihazı müəyyən edən ünvandır. Host ünvanı host hissəsinin bitlərinin hamısı 0-a təyin edilmədikdə əldə edilir. Məsələn, eyni 192.168.1.0/24 şəbəkəsində host ünvanı 192.168.1.100 ola bilər. Multicast ünvanları şəbəkədəki aktiv cihazları müəyyən edir. Multicast trafik adətən eyni paketi bir neçə təyinat yerinə yetirməli olan multimedia proqramları tərəfindən istifadə olunur (şəkil 2.46).



Şəkil 2.46. Multicast ünvanlama rejimi

Broadcast şəbəkə ünvanı şəbəkədəki bütün cihazlara mesaj yayımlamaq üçün istifadə edilən ünvandır. IPv4-də yayım ünvanı bütün host bitləri 1-ə təyin edilmiş ünvandır. 192.168.1.0/24 şəbəkəsinin nümunəsində yayım ünvanı 192.168.1.255 olacaqdır. Translyasiya ünvanları Unicast və Multicast ünvanlarından fərqli olaraq, şəbəkədəki bütün hostları müəyyənləşdirir və məlumat paketlərini göndərir. Yayım trafiki alt şəbəkədəki bütün cihazlara göndərilir ki, bu da keçid sıxlığına səbəb ola bilər və şəbəkə performansını azalda bilər (Şəkil 2.47).



Şəkil 2.47. Multicast ünvanlama rejimi

IPv4 ünvanlama. IPv4 (İnternet Protokolu 4-cü versiya) İnternetdə cihazları müəyyən etmək və yönləndirmək üçün istifadə olunan əsas şəbəkə səviyyəsi protokoludur. IPv4 IP ünvanlarının formatını və strukturunu, həmçinin məlumat paketlərinin şəbəkədə marşrutlaşdırılması və çatdırılması mexanizmlərini müəyyən edən qaydalar və standartlar toplusudur. O, təxminən 4,3 milyard unikal IP ünvanı yaratmağa imkan verən 32 bitlik ünvanlardan istifadə edir.

IPv4 şəbəkədəki hər bir cihaza IP ünvanı şəklində unikal identifikator təyin edir. Bu ünvan 32 bitdən ibarətdir (adətən nöqtələrlə ayrılmış 0-dan 255-ə qədər dörd ədəd kimi təmsil olunur). Bir cihaz məlumat paketini şəbəkəyə göndərdikdə, paket başlığında alıcının IP ünvanını və öz IP ünvanını ehtiva edir. Şəbəkədəki marşrutlaşdırıcılar bu məlumatdan paketin təyinat yerinə çatmaq üçün keçməli olduğu yolu müəyyən etmək üçün istifadə edirlər.

IPv4 İnternetdə və yerli şəbəkələrdə şəbəkə bağlantısının təmin edilməsində əsas rol oynayır. Onun əsas vəzifələrinə aşağıdakılar daxildir:

- Unikal IP ünvanlarından istifadə edərək şəbəkədəki cihazları müəyyənləşdirir.
- Şəbəkədəki cihazlar arasında məlumat paketlərinin marşrutlaşdırılması və çatdırılması.
- HTTP, FTP, SMTP və s. kimi müxtəlif şəbəkə xidmətləri və protokolları üçün dəstək.
- Lokal şəbəkələrdə və qlobal İnternetdə ünvanlama və marşrutlaşdırmanın təmin edilməsi.

Geniş istifadəsinə baxmayaraq, IPv4 məhdud ünvan sahəsi və səmərəsiz ünvan istifadəsi də daxil olmaqla bəzi məhdudiyyətlərə malikdir. Bu, 128 bitlik ünvanlardan istifadə edən və daha böyük ünvan sahəsi təmin edən növbəti nəsil IPv6 protokolunun inkişafına səbəb oldu.

IPv4 Sinifləri. IPv4 orijinal protokol spesifikasiyasında təqdim edilmiş sinifli ünvanlama strukturuna malik idi, lakin indi köhnəlmişdir və istifadəsi tövsiyə edilmir (cədvəl 2.7). Cədvəldən göründüyü kimi, hər sinifin təsviri aşağıdakı kimidir:

A sinfi:

İnterval: 0.0.0.0 - 127.255.255.255

Ünvanın birinci baytı (okteti) sinfi müəyyən etmək üçün istifadə olunur və həmişə bit 0 ilə başlayır.

Xüsusiyyətlər: A sinfi çox sayda ünvan təmin etdi, lakin az sayda şəbəkə ilə (yalnız 128), hər birində çoxlu sayda cihaz ola bilər.

B sinfi:

İnterval: 128.0.0.0 - 191.255.255.255

Ünvanın birinci baytı 10 ilə başlayır, bu da B sinfini göstərir.

Xüsusiyyətlər: B sinfi A sinfindən daha az ünvan təmin etdi, lakin hər birində orta sayda cihaz ola bilən daha çox sayda (təxminən 16 000) şəbəkə var.

C sinfi:

İnterval: 192.0.0.0 - 223.255.255.255

Ünvanın ilk baytı 110 ilə başlayır, bu da C sinfini göstərir.

Xüsusiyyətlər: C sinfi ən az ünvanları təmin edirdi, lakin hər birində az sayda cihaz ola bilən çoxlu sayda (təxminən 2 milyon) şəbəkə ilə.

D sinfi (multicast):

İnterval: 224.0.0.0 - 239.255.255.255

Ünvanın ilk baytı D sinfini göstərən 1110 ilə başlayır.

Xüsusiyyətlər: Bu sinif məlumatların müəyyən bir qovşaqdan çox bir qrup cihazlara çatdırılmalı olduğu zaman multicast məlumat ötürülməsi üçün istifadə olunur.

E sinfi (ehtiyatda saxlanılır):

İnterval: 240.0.0.0 - 255.255.255.255

Ünvanın ilk baytı E sinfini göstərən 1111 ilə başlayır.

Xüsusiyyətlər: Bu sinif gələcək tədqiqat və təcrübələrdə istifadə üçün qorunur və şəbəkələrdə ümumi istifadə üçün nəzərdə tutulmur.

Cədvəl 2.7

IPv4 Ünvan Sinifləri

Sinif	Aparıcı Bitlər	Şəbəkə hissəsinin ölçüsü	Host hissəsinin ölçüsü	Şəbəkələrin sayı	Şəbəkəyə görə ünvanlar	Başlanğıc ünvanı	Son Ünvan
A	0	8 bit	24	128	16,777,216	0.0.0.0	127.255.255.255
B	10	16 bit	16	16,384	65,536	128.0.0.0	191.255.255.255
C	110	24 bit	8	2.097.152	256	192.0.0.0	223.255.255.255
D	1110	–	–	–	–	224.0.0.0	239.255.255.255
E	1111	–	–	–	–	240.0.0.0	225.255.255.255

IPv4-ün sinifli ünvanlama strukturunun ünvan sahəsinin səmərəsiz istifadəsi, çevikliyin olmaması və çoxlu sayda ünvana ehtiyac kimi

çatışmazlıqlar var idi. Buna görə də, mövcud təcrübə IPv4 ünvanlanmasına sinifsiz marşrutlaşdırma (CIDR - Classless Inter-Domain Routing) adlanan, şəbəkənin səmərəliliyini və çevikliyini artırmaq üçün ünvan sahəsinin daha kiçik alt şəbəkələrə bölündüyü sinifli yanaşmanın istifadəsini tövsiyə edir.

IPV6 ÜNVANLAMA[20]. IPv6 (Internet Protocol version 6) IPv4-ü əvəz etmək üçün nəzərdə tutulmuş İnternet protokolunun ən son versiyasıdır. IPv6 kompüter şəbəkələri üzərindən məlumatların marşrutlaşdırılmasını və çatdırılmasını təmin edən şəbəkə səviyyəsi protokoludur.

Onun əsas məqsədi IPv4 ünvan məkanı tükəndiyi üçün İnternetdə ünvanlardan daha səmərəli istifadəni təmin etməkdir. IPv6 ünvan sahəsini IPv4-də 32 bitdən 128 bitə qədər genişləndirərək İnternetin gələcək inkişafı üçün nəhəng ünvanlar hovuzunu təmin edir. IPv6, IPv4 ilə eyni şəkildə işləyir, lakin genişləndirilmiş ünvan sahəsi ilə. Əsas fəaliyyət prinsiplərinə ünvanlama və marşrutlaşdırma daxildir.

IPv6-da ünvanlanma qlobal miqyasda unikal ünvanlar, multicast ünvanlar, zəncir ünvanları və s. daxildir. IPv6 marşrutlaşdırılması OSPFv3, IS-IS, BGP kimi dinamik marşrutlaşdırma protokollarından istifadə etməklə, həmçinin marşrutlaşdırma məlumatı mübadiləsi üçün ICMPv6 (IPv4-ün ICMP-nin analoqu) istifadə etməklə həyata keçirilir.

IPv6 ünvanlama sinifləri[21]. IPv6 şəbəkə ünvanlanmasında aşağıdakıları təmin edir:

1. Genişləndirilmiş ünvan məkanının təmin edilməsi – IPv6-nın əsas məqsədi İnternetə qoşulmuş hər bir cihaz üçün çoxlu sayda ünvan təmin etməkdir.

2. Yeni texnologiyalara dəstək – IPv6 müxtəlif cihazları birləşdirmək üçün çoxlu sayda IP ünvanlarının tələb olunduğu IoT (Əşyaların İnterneti) kimi yeni texnologiyalara dəstək verməkdir.

3. Təkmilləşdirilmiş Təhlükəsizlik – IPv6 standart olaraq şəbəkə təhlükəsizliyini yaxşılaşdırmağa kömək edən IPsec (IP Təhlükəsizliyi) kimi təhlükəsizlik xüsusiyyətlərini ehtiva edir.

---

[20] https://www.howtonetwork.com/comptia-network-study-guide-free/

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. М.: Форум,

[21] http://www.howtogeek.com/173921/secure-your-wireless-router-8-things-you-can-do-right-now/

4. Təkmilləşdirilmiş Performans – IPv6 şəbəkə performansını yaxşılaşdırmaq üçün sadələşdirilmiş başlıq və multicast rabitə dəstəyi kimi müxtəlif mexanizmlərdən istifadə edir.

Ümumilikdə, IPv6 qoşulmuş cihazların və xidmətlərin sayı artmaqda davam etdikcə İnterneti daha səmərəli və etibarlı etmək üçün nəzərdə tutulub.

Cədvəl 2.8-da IPv6 ünvan sinifləri təsvir olunmuşdur.

Cədvəl 2.8.
IPv6 Ünvan sinifləri

Ünvan növü	**Aralığı**	**Təsvir**
Qlobal Unicast Ünvanlar	2000::/3	Bu ünvanlar ictimai IPv4 ünvanlarına bənzəyir. Onlar qlobal İnternetdə qovşaqlar arasında ünsiyyət üçün nəzərdə tutulmuşdur.
Multicast Ünvanları	FF00::/8	Bu ünvanlar məlumat paketlərinin bir qrup qovşaqlara göndərildiyi multicast rabitəsi üçün istifadə olunur.
Link-Lokal Ünvanlar	FE80::/10	Bu ünvanlar yalnız bir şəbəkə seqmentində (məsələn, eyni kabel və ya simsiz kanalda) ünsiyyət qurmaq üçün nəzərdə tutulub. Onlar hər bir interfeysin yerli şəbəkədə unikal ünvana malik olmasını təmin edirlər.
Unikal Lokal Ünvanlar	FC00::/7	"Sayt-Lokal Ünvanlar" adlanan bu ünvanlar təşkilatların İnternetdə yönləndirilməməsi lazım olan lokal şəbəkələrində istifadə üçün nəzərdə tutulub.
Geri dönmə ünvanları	::1/128	IPv4 kimi, bu ünvanlar hostun şəbəkə yığınını yoxlamaq üçün istifadə olunur.

ŞƏBƏKƏ PROBLEMLƏRİNİN ARADAN QALDIRILMASI

Şəbəkədə nasazlıqların aradan qaldırılması mürəkkəb bir proses ola bilər, lakin müəyyən addımlar və üsullara əməl etməklə bunu çox sadə şəkildə yerinə yetirmək olar. Şəbəkə problemlərinin aradan qaldırılması üçün standart olaraq aşağıdakı qaydalardan istifadə olunur:

- Şəbəkə arxitekturasının təhlili.
- Şəbəkə yardım proqramlarından istifadə.
- Fiziki əlaqələrin yoxlanması.
- IP ünvanının yoxlanılması.
- Hadisə jurnalının təhlili.
- Avadanlığın yenilənməsi və yenidən yüklənməsi.
- Problemin təcrid edilməsi.
- Tövsiyyəedici sənədlər və ekspert rəyi.

Şəbəkənin problemlərini uğurla həll etmək üçün müəyyən addımlara və üsullara əməl etmək vacibdir. Şəbəkə arxitekturasını təhlil etməklə başlamaq lazımdır. Şəbəkə strukturunuzu və cihazların bir-biri ilə necə əlaqə saxladığını anlamaq potensial problemləri tez bir zamanda müəyyən etməyə kömək edə bilər. Bura şəbəkənin xəritəsi, istifadə olunan protokollar və topologiya haqqında biliklər (ulduz, halqa və ya avtobus kimi) daxildir.

Uzaqdan yardım proqramlarından istifadə diaqnostikanı xeyli asanlaşdırır. Ping, traceroute, ipconfig/ifconfig və xüsusi trafik təhlili proqramı kimi alətlər hostun mövcudluğunu, gecikmə müddətini, marşrutları və digər şəbəkə parametrlərini yoxlamağa imkan verir. Bu, əlaqənin hansı nöqtədə baş verdiyini müəyyən etməyə kömək edir.

Fiziki əlaqələri yoxlamaq vacib bir addımdır. Buraya kabellərin, birləşdiricilərin və marşrutlaşdırıcılar və açarlar kimi şəbəkə cihazlarının yoxlanılması daxildir. Tez-tez problem düzəltmək asan olan boş və ya səhv birləşdirilmiş kabel ola bilər.

Cihazın IP ünvanını yoxlamaq tez-tez əlaqə problemlərinə səbəb olan ünvan konfliktlərini və ya yanlış konfiqurasiyaları aşkar edə bilər. Cihazın düzgün IP və marşrutlaşdırma parametrlərinə malik olduğundan və şəbəkədəki digər cihazlarla heç bir ziddiyyət olmadığından əmin olun.

Hadisə jurnalının təhlili problemlərin daha dərin səbəblərini müəyyən etməyə kömək edir. Qeydlərdə səhvlər, əlaqə nasazlıqları və ya ilk baxışdan aydın görünməyən digər problemlər haqqında qeydlər ola bilər. Bu, problemin

mənbəyini daha dəqiq müəyyən etməyə və müvafiq tədbirlər görməyə imkan verir.

Avadanlığın yenilənməsi və yenidən işə salınması tez-tez müvəqqəti şəbəkə kəsilməsini və xətaları aradan qaldırmağa kömək edir. Bəzən şəbəkə cihazının proqram təminatının yenilənməsi və ya yenidən başlaması heç bir əlavə səy göstərmədən problemi həll edə bilər.

Problemin təcrid olunması da əsas addımdır. Şəbəkənin hansı hissəsinin və ya hansı xüsusi cihazın problemlərə səbəb olduğunu müəyyən etmək problemi daraltmağa və səylərinizi xüsusi şəbəkə elementlərinə yönəltməyə kömək edir.

Nəhayət, rəhbər sənədlərə və ekspert rəylərinə etibar etmək vacibdir. Avadanlıq istehsalçılarının təlimatlarından və tövsiyələrindən istifadə etmək, həmçinin mürəkkəb halları təhlil etmək üçün mütəxəssisləri işə götürmək problemi tez tapmağa və həll etməyə kömək edəcəkdir.

VİRTUALLAŞDIRMA TEXNOLOGİYALARI

Virtuallaşdırmanın əhəmiyyəti və tətbiqi virtual maşınlardan çox kənara çıxır. İnformasiya texnologiyalarında heç bir irəliləyiş virtuallaşdırma qədər dəyərli olmamışdır. Bir çox İT mütəxəssisləri virtuallaşdırmanı virtual maşınlar (**VM**) və onlarla əlaqəli hipervizorlar və əməliyyat sistemləri baxımından düşünür, lakin bu, aysberqin yalnız görünən tərəfidir. Getdikcə daha geniş virtuallaşdırma texnologiyaları, strategiyaları və imkanları bütün dünyada təşkilatlarda İT-nin əsas elementlərini yenidən müəyyənləşdirir.

Virtuallaşdırma[22] aparat tətbiqindən mücərrədləşdirilmiş hesablama resursları toplusunun və ya onların məntiqi birləşməsinin təmin edilməsi və eyni zamanda eyni fiziki resursda işləyən hesablama proseslərinin bir-birindən məntiqi təcrid olunmasıdır. Məsələn, Server infrastrukturunun təşkilinə

22

İsmayıl Calallı (Sadıqov), "İnformatika terminlərinin izahlı lüğəti", 2017, "Bakı" nəşriyyatı, 996 s.
Mark Ciampa. CompTIA® Security+ Guide to Network Security Fundamentals, Seventh EditionCengage Learning, Inc. 2022, WCN: 02-300
Principles of Information Security, 7th Edition Michael E. Whitman and Herbert J. Mattord
Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.
Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. Издательство Политехнического университета, Санкт-Петербург, 2005.

ənənəvi yanaşma hər bir proqram üçün ayrıca fiziki serverdən istifadə etməyi nəzərdə tutur. Bu, belə bir tətbiqin pik yüklənmə zamanı lazımi hesablama resurslarına malik olacağına zəmanət verməyə, həmçinin bir tətbiqin uğursuzluğu digərlərinin işinə təsir göstərməməsi üçün bu proqramı digərlərindən təcrid etməyə imkan verir. Bununla belə, belə bir strategiya fiziki serverlərin sayının xətti artımı və nəticədə avadanlıqların alınması və istismarı xərclərinin artması ilə əlaqələndirilir. Eyni zamanda, server avadanlığından istifadə üçün belə bir sxem ilə hesablama gücünün orta istifadəsi 10% -dən çox deyil ki, bu da açıq bir tullantı kimi görünür. Məsələn, Microsoft Active Directory domen nəzarətçisi və İnternet şlüzünü eyni fiziki serverdə birləşdirməyi qəti şəkildə rədd edir, çünki bu, ciddi təhlükəsizlik riski yaradır. Müvafiq olaraq, bir çox sistem administratorları domen nəzarətçisini bir fiziki serverə, İnternet şlüzünü isə digərinə yerləşdirir. Burada bir problem yaranır: hər bir fərdi server pula başa gəlir, elektrik enerjisi istehlak edir və masada və ya rafda yer tutur. Bu, serverlər üçüncü tərəfin məlumat mərkəzində yerləşdiyi təqdirdə xüsusilə vacib olur, burada onlar rəflərdəki işğal edilmiş bölmələr üçün ödəniş alırlar və enerji istehlakı ciddi şəkildə məhdudlaşdırılır. Hər bir belə tapşırıq üçün ayrıca serverdən istifadə etmək məntiqsiz görünür. Server infrastrukturunun virtuallaşdırılması bu problemi həll etməyə imkan verir. Virtuallaşdırmanın üstünlüklərinə daxildir:

- Server konsolidasiyası.
- Artan etibarlılıq.
- Klasterləşmə.
- İnfrastrukturun asan idarə edilməsi.

Biznes proqramlarının virtuallaşdırılması hər bir tətbiqi öz serverinə ayırmaq əvəzinə, birdən çox proqramı tək fiziki serverdə (host) işə salmağa imkan verir. İndi təşkilatın işə salması lazım olan bütün proqramlar daha az serverdə işləyə bilər. Serverin konsolidasiyası server infrastrukturunun saxlanması xərclərini 50-60% azaltmağa imkan verir. Virtuallaşdırma həmçinin tətbiqlərin etibarlılığını və ğursuzluqlara qarşı dayanıqlığını əhəmiyyətli dərəcədə artıra bilər. Serverlərdən biri uğursuz olarsa, onda yerləşdirilən virtual maşınlar avtomatik olaraq başqa serverdə yenidən işə salına və işləməyə davam edə bilər. Üstəlik, davamlı işləməli olan kritik missiya tətbiqləri üçün müxtəlif fiziki serverlərdə iki virtual maşın yarada bilərsiniz - əsas və onun güzgü nüsxəsi. Əsas virtual maşın uğursuz olarsa, onun güzgü nüsxəsi tətbiqin davamlılığını təmin edəcəkdir. Virtual maşınlarla işləyən bir neçə fiziki server (host) klasterdə birləşdirilə bilər. Klasterdəki bütün serverlərin aparat

resursları klasterin virtual maşınları tərəfindən paylaşıla bilən ümumi resurs hovuzunu təşkil edir. Virtuallaşdırma proqramı, işləyən virtual maşınları daha çox yüklənmiş serverlərdən daha az yüklənmiş olanlara köçürərək, klasterin bir hissəsi olan serverləri balanslaşdırmağa imkan verir. Klasterdə ümumi yük azalarsa (məsələn, gecə), virtual maşınlar avtomatik olaraq az sayda serverdə "toplana" bilər və qalan serverlər söndürüləcəkdir.

İnfrastrukturun asan idarə edilməsi 2 prinsip üzərindən təşkil olunur:

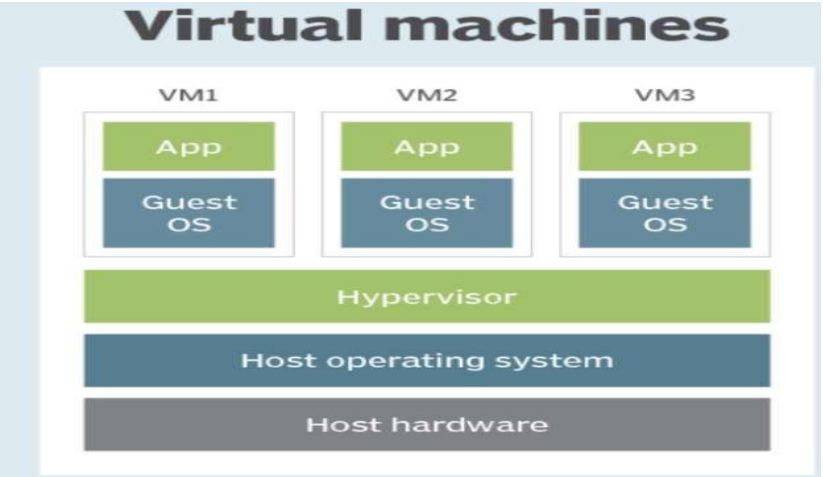
Sürətli yerləşdirmə. Yeni serverin yerləşdirilməsi bir qədər vaxt aparır. Buraya OS-nin quraşdırılması, sürücülərin quraşdırılması, proqramların quraşdırılması və s. daxildir. Virtual maşınlarla hər şey sadədir: bir neçə siçan klikləməklə virtual maşının tamamilə eyni "klonlarını" yarada bilərsiniz və proses təxminən bir neçə dəqiqə çəkəcək.

Yedəkləmələr. Bir ehtiyat nüsxəsi hazırlansa belə, OS-ni ondan çılpaq metala bərpa etmək mümkün olacağına və səhvsiz işləyəcəyinə 100% zəmanət vermək həmişə mümkün deyil. Xüsusilə hardware konfiqurasiyası əvvəlkindən bir qədər fərqlidirsə. Virtual maşınlarda bütün aparat təqlid edilir və buna görə də standartdır və tam ehtiyat nüsxəsi üçün sadəcə bir və ya bir neçə faylı kopyalamalısınız. Bərpa etmək üçün sadəcə fayl(lar)ı virtualizasiya mühiti olan host ƏS-nin artıq quraşdırıldığı yeni serverə köçürməli və onları "götürməlisiniz" və virtual maşın heç nə olmamış kimi işləyəcək.

Virtuallaşdırma obyektləri. Virtuallaşdırma kontekstində obyektlər virtual mühit yaratmaq üçün virtuallaşdırılan resurslar və ya komponentlərdir. Virtuallaşdırma obyektləri virtuallaşdırmanın növündən asılı olaraq fərqlənə bilər, lakin onlara adətən aşağıdakılar daxildir:

- Virtual Maşınlar (VM).
- Konteynerlər.
- Virtual şəbəkələr.
- Virtual Yaddaş.
- Verilənlər bazası.

Virtual Maşınlar (VM) fiziki serverin üstündə işləyən virtuallaşdırılmış kompüterlərdir. Onların öz virtual prosessorları, yaddaşı, disk sahəsi və şəbəkə interfeysləri var. VM-lər birdən çox təcrid olunmuş əməliyyat sistemini tək fiziki serverdə işə salmağa imkan verir ki, bu da aparat resurslarından istifadənin səmərəliliyini artırır. Virtual maşın həm proqram təminatında, həm də aparatda həyata keçirilə bilər. Virtual maşın hardware təqlid edir (şəkil 2.48).



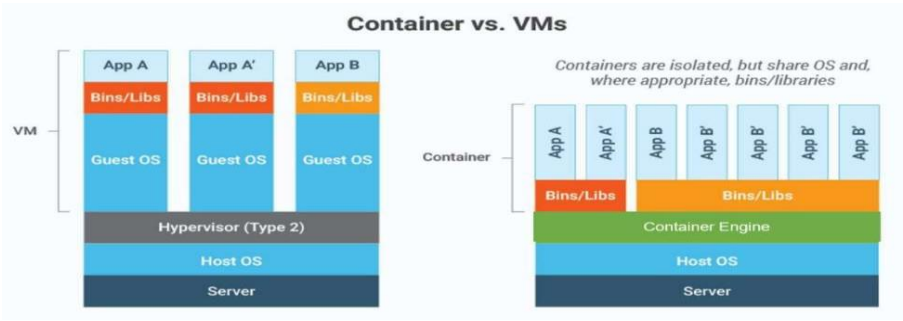
Şəkil 2.48. Virtual maşın

Prosessordan əlavə, VM həm fərdi aparat komponentlərinin, həm də bütün real kompüterin (o cümlədən BIOS, RAM, sərt disk və digər periferik qurğuların) işini təqlid edə bilər. Sonuncu halda, əməliyyat sistemləri real kompüterdə olduğu kimi VM-də quraşdırıla bilər (məsələn, Windows Linux altında virtual maşında və ya əksinə işlədilə bilər). Qonaq ƏS virtual maşın daxilində işləyən əməliyyat sistemidir.Virtual maşınlar hosting platformasında yerləşdirilir. Host platforması - host platforması, host platforması. Bir hostda bir neçə virtual maşın işləyə bilər.

Hipervisor adlanan nazik proqram təbəqəsi virtual maşınları serverdən ayırır və lazım olduqda hər bir virtual maşına hesablama resurslarını dinamik şəkildə ayırır.

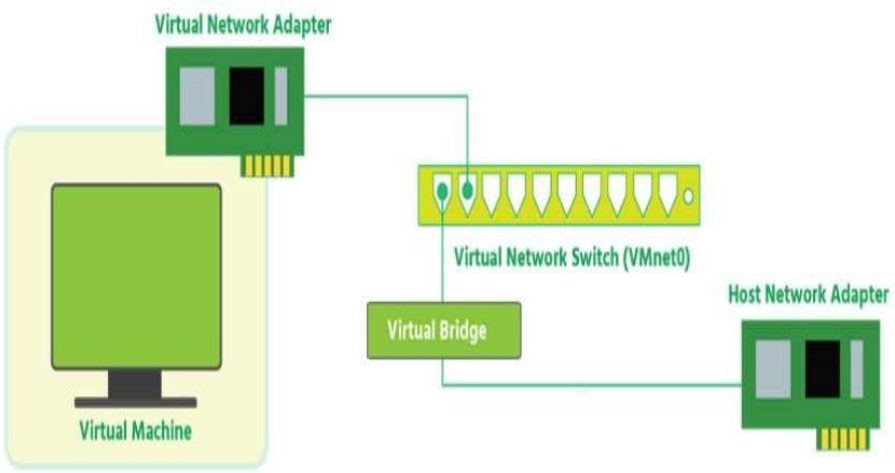
Virtual maşınları quraşdırma proqramları kimi əməliyyat sistemlərinin parametrlərinə təsir edən virtual maşınlarda tətbiqləri sınaqdan keçirmək rahatdır. Virtual maşınların yerləşdirilməsinin asanlığına görə, onlar tez-tez yeni məhsul və texnologiyaların öyrədilməsi üçün istifadə olunur. Bir çox proqram tərtibatçıları əvvəlcədən quraşdırılmış məhsullarla virtual maşınların hazır şəkillərini yaradır və onları pulsuz və ya kommersiya əsasında təqdim edirlər.

Konteynerlər tətbiqlərin və onların asılılıqlarının işləyə biləcəyi virtuallaşdırılmış mühitlərdir. Onlar ümumi əməliyyat sistemində işləyirlər və müstəqillik və təhlükəsizliyi təmin etmək üçün resurs izolyasiyasından istifadə edirlər. Konteynerlər yüngüldür və sürətli işə salınma vaxtlarına malikdir, bu da onları mikroservis arxitekturaları və bulud-doğma tətbiqlər üçün ideal seçim edir (şəkil 2.49).



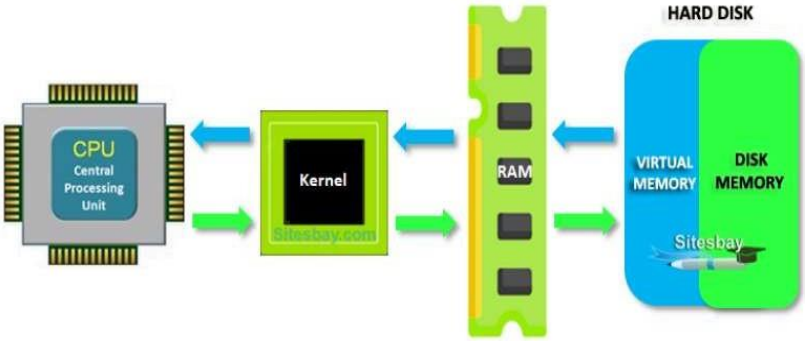
Şəkil 2.49. Konteynerlər

Virtual şəbəkələr fiziki infrastrukturun üzərində qurula bilən virtuallaşdırılmış şəbəkə mühitləridir. Onlar ayrı şəbəkə seqmentləri, virtual LAN və VPN əlaqələri yaratmağa imkan verir. Virtual şəbəkələr şəbəkə konfiqurasiyasını idarə etməyi və müxtəlif şəbəkə cihazları arasında trafiki təhlükəsiz şəkildə ayırmağı asanlaşdırır (şəkil 2.50).



Şəkil 2.50. Virtual şəbəkə

Virtual yaddaş fiziki disklərdən və RAID massivlərindən abstraksiyadır. Onlar müxtəlif fiziki mağazalardan yaradıla bilər və məlumat anbarlarının idarə edilməsində və miqyasında çeviklik təmin edir. Virtual yaddaş kosmosun dəqiq tənzimlənməsi, artıqlıq, anlıq görüntülər və replikasiya kimi funksiyaları təmin edərək onu məlumatların idarə edilməsi üçün əlverişli alətə çevirir (şəkil 2.51)



Şəkil 2.51. Virtual yaddaş

Verilənlər bazası. Verilənlərin virtualizasiyası verilənlərin əsasını təşkil edən idarəetmə və saxlama sistemlərindən, habelə onların strukturundan asılı olmayaraq məlumatların mücərrəd formada təqdim edilməsidir. Bu, tətbiqlərin, hesabat alətlərinin və son istifadəçilərin orijinal mənbələr, yerlər və məlumat strukturları haqqında ətraflı biliyə ehtiyac olmadan məlumat əldə edə bilməsi üçün bir səviyyədə birdən çox mənbədən verilənləri birləşdirməyə yanaşmadır.

Bu virtuallaşdırma obyektləri istifadəçilərə aparat resurslarından səmərəli istifadə edə bilən və İT infrastrukturunun idarə edilməsini sadələşdirən çevik, genişlənən və yüksək performanslı virtual mühitlər yaratmağa imkan verir.

Virtual maşınların əsas xüsusiyyətləri aşağıdakılardır:

1. **İnkapsulyasiya.** Virtual maşın virtual aparat, qonaq ƏS və proqramların tam dəsti olan proqram kompüteridir. Söndürüldükdə virtual maşın adi fayllar toplusu kimi diskə yazılır (inkapsulyasiya olunur), işə salındıqda isə bu dəstdən oxunur. İnkapsulyasiya sayəsində virtual maşınları asanlıqla başqa fiziki serverə köçürmək, klonlaşdırmaq və ya istənilən saxlama qurğusuna ehtiyat nüsxəsini çıxarmaq olar. Bir uğursuzluqdan sonra virtual maşını bərpa etmək üçün əməliyyat sistemini və proqramları yenidən quraşdırmaq lazım deyil, sadəcə onu ehtiyat nüsxədən yenidən başlatmalısınız.

2. **İzolyasiya.**Bir neçə virtual maşın bir fiziki serverdə birlikdə işlədikdə, onlar bir-birindən tamamilə təcrid olunurlar. Bu o deməkdir ki,

a) hər bir VM yalnız ona ayrılmış aparat resurslarının bir hissəsindən istifadə edə bilər və nəticədə digər virtual maşınların işinə təsir göstərmir

b) VM-lər bir-birindən asılı olmayaraq işləyir, ona görə də maşınlardan biri proqram xətası səbəbindən sıradan çıxsa belə, digər maşınların işi pozulmayacaq.

3. **Uyğunluq.** Aparat konfiqurasiyası çox fərqli ola bilən fiziki kompüterlərdən fərqli olaraq, virtual maşınlar virtual "hardware" komponentlərinin standart dəstini ehtiva edir. Nəticədə, virtual maşınlar x86 platforması üçün bütün ümumi əməliyyat sistemləri və proqramları ilə tam uyğun gəlir. Əməliyyat sistemlərində və ya proqramlarda heç bir dəyişiklik tələb olunmur.

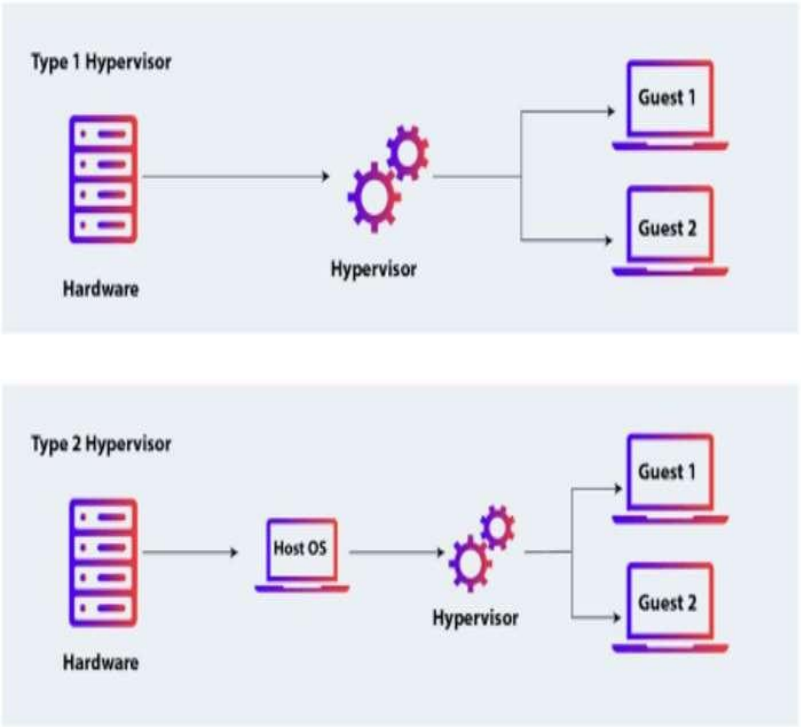
4. **Avadanlığın müstəqilliyi.** Virtual maşınlar fiziki aparatda deyil, hipervizor mühitində işlədiyi üçün həmin aparatın konfiqurasiyasından tamamilə müstəqildirlər. Buna görə də, virtual maşınlar, əməliyyat sistemləri, tətbiqləri və virtual qurğu drayverləri ilə birlikdə heç bir dəyişiklik edilmədən bir fiziki serverdən tamamilə fərqli aparat konfiqurasiyasına malik digər fiziki serverə ötürülə bilər.

Hipervizorlar. Hipervisor virtuallaşdırma konsepsiyasının arxasında duran hərəkətverici qüvvədir, fiziki host kompüterə qonaq əməliyyat sistemləri kimi çoxsaylı virtual maşını idarə etməyə imkan verir ki, bu da öz növbəsində yaddaş, şəbəkə bant genişliyi və prosessor dövrləri kimi hesablama resurslarından maksimum istifadə etməyə kömək edir.

Hipervizor eyni əsas kompüterdə bir neçə əməliyyat sisteminin eyni vaxtda paralel icrasını təmin edən və ya imkan verən proqram və ya aparat sxemidir. Hipervisor həmçinin əməliyyat sistemlərinin bir-birindən təcrid olunmasını, mühafizə və təhlükəsizliyi, müxtəlif işləyən ƏS-lər arasında resurs mübadiləsini və resursların idarə edilməsini təmin edir. Hipervisor həm proqram, həm də aparatda həyata keçirilə bilər. Hipervizorun özü müəyyən mənada minimal əməliyyat sistemidir (mikrokernel və ya nanokernel). Hipervisor virtual maşınların və onların qonaq əməliyyat sistemlərinin işləməsini təmin edir. Onun nəzarəti altında işləyən əməliyyat sistemlərinə virtual maşın xidməti təqdim edir, konkret maşının real (fiziki) aparatını virtuallaşdıran və ya təqlid edir. Hipervisor qonaq əməliyyat sistemlərini bir-birindən təcrid edir. Bu, müəyyən bir OS ilə işləyən virtual maşınlardan hər hansı birini müstəqil olaraq "yandırmağa", yenidən işə salmağa, "söndürməyə" imkan verir. Hipervisor hostun resurslarını idarə edir. Virtual maşınlar üçün resursları ayırır və buraxır. Hipervizor eyni zamanda eyni əsas kompüterdə onun nəzarəti altında işləyən ƏS-ləri, sanki ƏS-lər müxtəlif fiziki kompüterlərdə

işləyirmiş kimi bir-biri ilə ünsiyyət və qarşılıqlı əlaqə vasitələri ilə (məsələn, fayl mübadiləsi və ya şəbəkə əlaqələri vasitəsilə) təmin edə bilər.

Hipervizorların növləri. Hipervizorlar IBM tərəfindən özünün əsas sistem sistemlərindən istifadə etmək üçün hazırlanmış və sonradan fərdi kompüterlərə və serverlərə əlavə edilmiş hardware virtualizasiyasının əsas komponentinə çevrilmişdir. VMware xərcləri idarə etmək üçün daha çox funksiya və seçim təmin etməklə Linux və Unix sistemlərini daha yaxşı edir. Bugünkü hipervizorlar iki əsas növdə mövcuddur (şəkil 2.52).

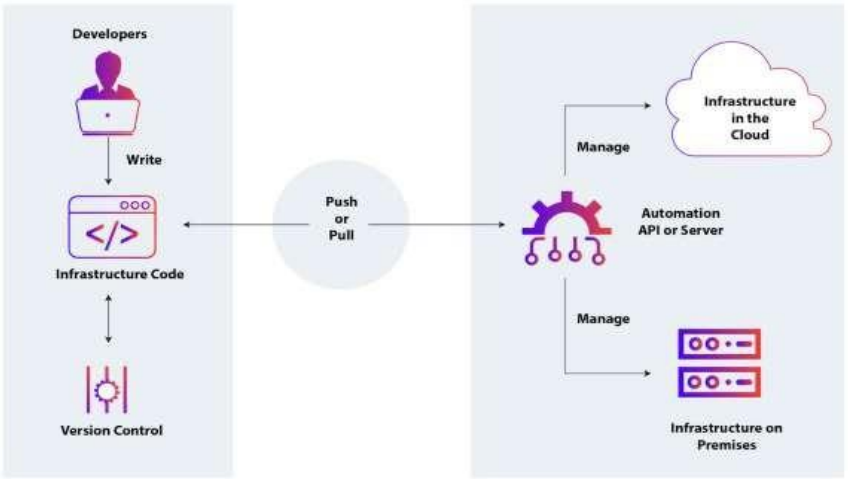


Şəkil 2.52. Hipervizorların növləri

1-ci tip hipervizorlar kimi tanınan çılpaq metal hipervizorları çılpaq metal hostinq üçün istifadə olunur. Onlar əməliyyat sistemindən istifadə etmədən birbaşa müştərinin kompüterində işləyirlər. Onlar virtual mühiti idarə etmək və idarə etmək üçün ayrıca maşın tələb edir. Yüksək dərəcədə qorunan virtuallaşdırma sistemləri yalnız o halda işləyir ki, hipervizorun daxilində işləyən əməliyyat sistemi (ƏS) fiziki avadanlığa birbaşa çıxışı varsa, aralarında hücum zamanı təhlükə yarada biləcək heç bir şey yoxdur. Konteynerlərlə VM-lərdən daha çox şey mümkündür. Hypervisor texnologiyası təkmilləşdirilmiş

məlumatların qorunması, məlumatların suverenliyi və artan virtual maşın sıxlığı kimi mühüm müəssisə üstünlükləri təklif edir. Serverlər kimi, Tip 1 hipervizorlar masaüstü əməliyyat sistemlərini virtuallaşdıra bilirlər. Virtual Masaüstü İnfrastruktur VDI həllinin əsasını təşkil edir ki, bu da sizə mərkəzi serverdə virtual maşınlar daxilində işləyən Windows və ya Linux iş masası mühitlərinə daxil olmağa imkan verir. Bağlantı brokeri vasitəsilə hipervizor hovuzdan virtual iş masasını şəbəkə üzərindən ona daxil olan bir istifadəçiyə təyin edir və istənilən cihazdan uzaqdan işləməyə imkan verir. Siz yerli serverdən və ya buluddan sizə fiziki iş masasının funksionallığını verəcək tam funksional virtual masaüstləri təqdim etmək üçün Citrix VDI həllərindən istifadə etmək olar.

Tip 2 hipervizorlar, həmçinin hosted hipervizorlar adlanır, əməliyyat sistemi daxilində proqram kimi işləyirlər (şəkil 2.53).



Şəkil 2.53. Tip 2 hipervizorlar

Virtual maşın hər hansı digər proqram kimi öz funksiyasını yerinə yetirmək üçün əsas əməliyyat sistemindən tələb edir. Qonaq və ev sahibini ayırmağa imkan verən eyni yaddaş seqmentində işləmək məcburiyyətində deyil. Çoxsaylı Tip 2 hipervizorlar tək host əməliyyat sisteminin üstündə işləyə bilər və hər hipervizorun özündə birdən çox əməliyyat sistemi ola bilər. Virtuallaşdırma texnologiyası bank, sığorta, istehsal, tikinti, pərakəndə satış, təhsil, nəqliyyat, səhiyyə və hökumət daxil olmaqla müxtəlif bizneslər üçün

ideal həll yoludur.

YOXLAMA SUALLARI

1. Aktiv və passiv şəbəkə cihazları hansılardır?
2. Aktiv və passiv şəbəkə cihazları arasında fərq nədir?
3. Aktiv və passiv şəbəkə cihazlarının bəzi nümunələri hansılardır?
4. OSI modeli hansı səviyyələri əhatə edir?
5. TCP/IP modeli hansı səviyyələri əhatə edir?
6. OSI modeli ilə TCP/IP modeli arasındakı əsas fərq nədir?
7. OSI model təbəqələrinin məlumat ötürülməsi prosesində rolu nədir?
8. OSI modelinin hər səviyyəsinəi hansı şəbəkə cihazları və texnologiyaları uyğun gəlir?
9. OSI modelinin müxtəlif səviyyələrində olan şəbəkə komponentləri bir-biri ilə necə qarşılıqlı əlaqədə olur?
10. IP ünvanı nədir və şəbəkədəki hər bir cihaz üçün necə unikaldır?
11. IP protokolunun hansı versiyaları var və onların fərqi nələrdir?
12. IPv4 və IPv6 ünvanlarının strukturu necədir?
13. Şəbəkələr kontekstində marşrutlaşdırma və kommutasiya nədir?
14. Şəbəkədə məlumatların ötürülməsi yolunu müəyyən etmək üçün hansı marşrutlaşdırma protokollarından istifadə olunur?
15. Hansı kommutasiya texnologiyaları mövcuddur və onların fərqləri nələrdir?
16. Şəbəkə bağlantılarında port nömrələri niyə lazımdır?
17. Müxtəlif şəbəkə protokolları üçün hansı məşhur portlar ən çox istifadə olunur?
18. Hansı proqramlar standart TCP və UDP portlarından istifadə edir?
19. Şəbəkə problemlərinin diaqnostikası və aradan qaldırılması üçün hansı üsullardan istifadə etmək olar?
20. Cihazın və ya xidmətin şəbəkədə niyə əlçatan olmadığını necə müəyyən edə bilərik?
21. Şəbəkə virtualizasiyası nədir və onu həyata keçirmək üçün hansı texnologiyalardan istifadə olunur?
22. Şəbəkə virtualizasiyasının üstünlükləri və mənfi cəhətləri hansılardır?

PRAKTİKİ TAPŞIRIQ

1. Routerin quraşdırılması.

Tapşırıq: Routerin statik və ya dinamik IP ünvanı vasitəsilə İnternetə qoşulmaq üçün konfiqurasiya edin.

Məqsəd: İnterfeys IP ünvanları, standart marşrutlar və marşrutlaşdırma protokolları kimi əsas marşrutlaşdırıcı parametrlərinin konfiqurasiya prosesini öyrənmək.

2. Switch quraşdırması

Tapşırıq: Kommutatorda virtual yerli şəbəkə (VLAN) yaradın və müxtəlif VLAN-larda işləmək üçün portları konfiqurasiya edin.

Məqsəd: Şəbəkəni məntiqi qruplara bölmək və trafiki idarə etmək üçün keçidin konfiqurasiyası prosesi ilə tanış olmaq.

3. Şəbəkə problemlərinin diaqnostikası.

Məqsəd: Şəbəkədəki hostun niyə əlçatmaz olduğunu müəyyən etmək üçün ping, tracert və ipconfig/ifconfig kimi şəbəkə problemlərinin həlli alətlərindən istifadə edin.

Məqsəd: Standart əməliyyat sistemi alətlərindən istifadə etməklə şəbəkə problemlərinin təhlili və onların həlli üsullarını mənimsəmək.

4. Şəbəkədə OSI modelindən və TCP/IP protokolundan istifadə

Tapşırıq: Kiçik ofis üçün OSI modelindən və TCP/IP protokolundan istifadə edərək şəbəkə infrastrukturu yaradın.

Məqsəd: Standart modellər və protokollardan istifadə edərək şəbəkənin layihələndirilməsi və konfiqurasiyası prosesini mənimsəmək.

5. Şəbəkə proqramının hazırlanması

Tapşırıq: TCP/IP protokol yığınından istifadə edərək sadə şəbəkə proqramı yazın.

Məqsəd: Şəbəkə üzərindən verilənlərin ötürülməsinin əsas prinsiplərini, proqramların şəbəkə protokolları ilə qarşılıqlı əlaqəsini və şəbəkə məlumatlarının işlənməsini başa düşmək.

6. VPN serverinin qurulması

Tapşırıq: İnternet vasitəsilə korporativ şəbəkəyə təhlükəsiz uzaqdan girişi təmin etmək üçün VPN serverini konfiqurasiya edin.

Məqsəd: Təhlükəsiz uzaqdan girişi təmin etmək üçün virtual şəxsi şəbəkələrin (VPN) qurulması və istifadəsi prosesini mənimsəmək.

7. Host-A-da IPv4 ünvanı və 10.5.4.100 255.255.255.0 alt şəbəkə maskası var. Host-A şəbəkə ünvanı hansıdır?

10.0.0.0
10.5.0.0
10.5.4.0
10.5.4.100

8. Host-A-da IPv4 ünvanı və 172.16.4.100 255.255.0.0 alt şəbəkə maskası var. Aşağıdakı IPv4 ünvanlarından hansı Host-A ilə eyni şəbəkədə olacaq? (Tətbiq olunanların hamısını seçin).

172.16.4.99
172.16.0.1
172.17.4.99
172.17.4.1
172.18.4.1

9. Host-A-da IPv4 ünvanı və 192.168.1.50 255.255.255.0 alt şəbəkə maskası var. Aşağıdakı IPv4 ünvanlarından hansı Host-A ilə eyni şəbəkədə olacaq? (Tətbiq olunanların hamısını seçin).

192.168.0.1
192.168.0.100
192.168.1.1
192.168.1.100
192.168.2.1

10. Şəbəkə ünvanını müəyyən etmək üçün (ikilik və onluq formatda) AND əməliyyatından istifadə edin.

Qovşaqların ünvanı	**10**	**79**	**50**	**106**
Altşəbəkə maskası	255	255	0	0
İkilik formatda qovşaqların ünvanı	00001010	01001111	00110010	01101010
İkilik formatda Altşəbəkə maskası	11111111	11111111	00000000	00000000
İkilik formatda şəbəkə ünvanı				
Onluq formatda şəbəkə ünvanı				

MODUL 3. ŞƏBƏKƏ TOPOLOGİYASI

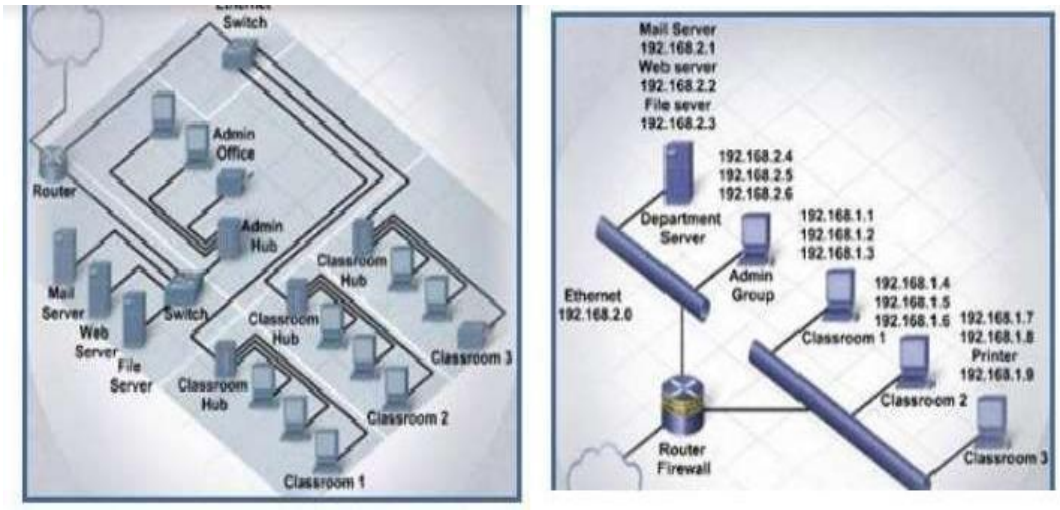
ŞƏBƏKƏ DİZAYNI VƏ TOPOLOGİYALAR
FİZİKİ BAĞLANTI PROBLEMLƏRININ ARADAN QALDIRILMASI
ETHERNET STANDARTLARI
NAQİLLƏRİN PAYLANMASI TEXNOLOGİYASI

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

ŞƏBƏKƏ DİZAYNI VƏ TOPOLOGİYALAR

Şəbəkə dizaynı[23]. Şəbəkə topologiyası şəbəkədəki cihazların bir-birinə qoşulma üsulunu təyin edən şəbəkənin struktur təşkili və ya konfiqurasiyasıdır. O, cihazların, kompüterlərin və digər şəbəkə komponentlərinin bir-birinə qoşulduğu və qarşılıqlı əlaqədə olduğu fiziki və ya məntiqi formanı təsvir edir. Şəbəkə topologiyasının 2 forması mövcuddur (şəkil 3.1):

1. Fiziki topologiya.
2. Məntiqi topologiya.



a)Fiziki topologiya b) Məntiqi topologiya

Şəkil 3.1. Şəbəkə topologiyasının formaları

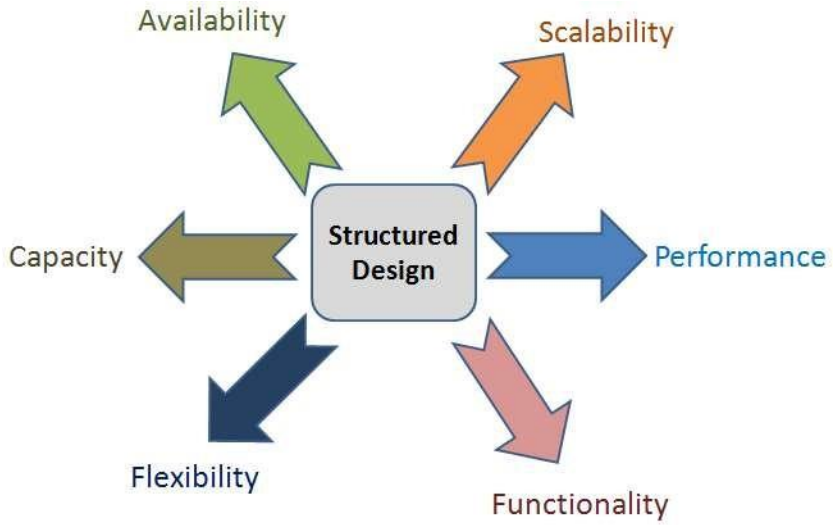
Şəkildən göründüyü kimi, fiziki topologiya kabellərin və şəbəkə avadanlığının şəbəkədə faktiki yerləşməsini müəyyən edir. Fiziki topologiyaya aşağıdakı strukturlar daxildir: Nöqtədən-Nöqtəyə (Point to Point), Tor (Mesh), Ulduz (Star), Şin (Bus), Ring (Halqa), Ağac (Tree), Hibrid (Hybrid).

[23] Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.
Келдыш Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. С.100
Пушнин А.В. Информационные сети и телекоммуникации / А.В.Пушнин, В.В.Янушко. Таганрог: Изд-во ТРТУ, 2015. 128

Fiziki topologiyada sistemli yanaşmadan istifadə edərək, şəbəkənin dizayn həlləri formalaşdırılır. Sistemli yanaşmanın tətbiqində əsas məqsəd yaradılan şəbəkə infrastrukturunun aşağıdakı tələblərə cavab verməsini təmin etməkdir (şəkil 3.2):

- Performans.
- Funksionallıq.
- Çeviklik.
- Tutum.
- Mövcudluq.
- Ölçüləbilənlik.

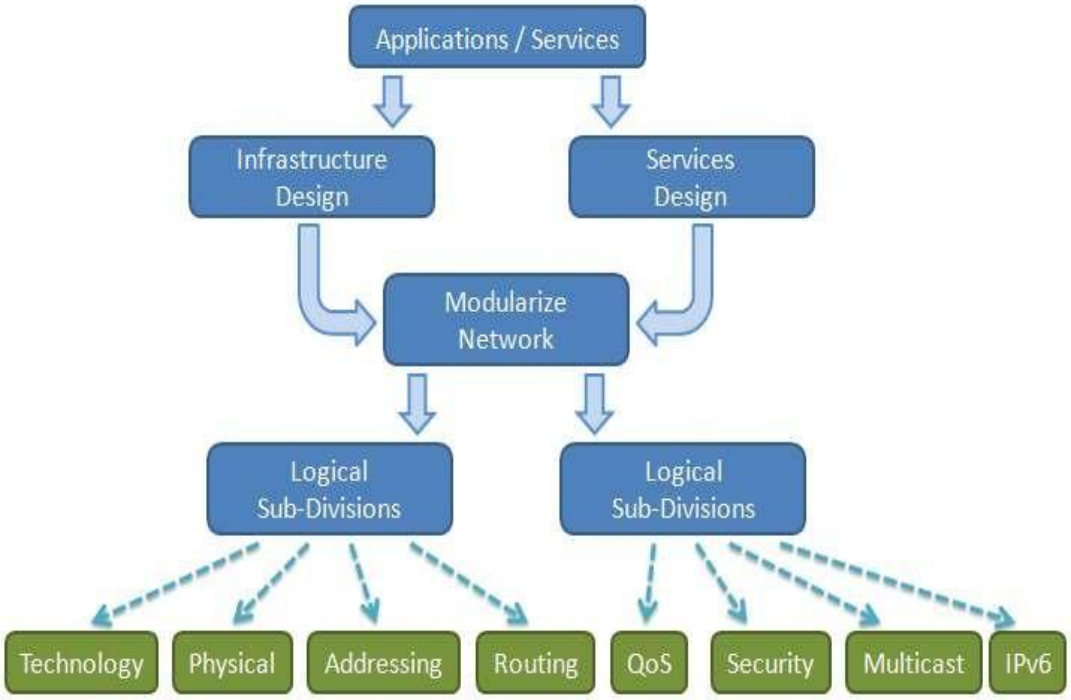
Dizayn həllərinin əsas məqsədi biznes proseslərinin ehtiyaclarını, təşkilati məqsədləri, siyasət və prosedurları, texniki məqsədləri və məhdudiyyətləri, mövcud və gələcək şəbəkə infrastrukturunu nəzərə alan sistematik yanaşmanın inkişaf etdirilməsidir. Sistematik yanaşma şəbəkə infrastrukturundan asılı olaraq yuxarıdan aşağıya və ya aşağıdan yuxarıya təşkil oluna bilər.



Şəkil 3.2. Şəbəkə topologiyasının dizayn həlləri

Yuxarıdan aşağıya sistem yanaşması orta ölçülü şəbəkədən böyük ölçülü şəbəkə dizaynına qədər tövsiyə olunan metodologiyadır. Bu yanaşmadan istifadə edərək dizayn detallarına keçməzdən əvvəl istifadəçiyə böyük mənzərəni və dizaynın bütün aspektləri təqdim olunur. Bu, əsasən, OSI şəbəkə modelinin yeddinci səviyyəsindən başlamaq və daha sonra tətbiq

təviyyəsindən təqdimat səviyyəsinə, seans səviyyəsinə, nəqliyyat səviyyəsinə, şəbəkə səviyyəsinə, kanal səviyyəsinə və nəhayət, fiziki səviyyəsinə keçmək deməkdir. Şəkil 3.3-də yuxarıdan-aşağıya yanaşmanın infoloji sxemi təsvir olunmuşdur.



Şəkil 3.3. Yuxarıdan-aşağıya yanaşma

Şəkildən göründüyü kimi, sistem yanaşması ümumi sistemdən başlayır və onu daha kiçik komponentlərə və ya alt sistemlərə ayırır. Bu yanaşma sistemin dizaynında və inkişafında əvvəlcə ümumi tələbləri müəyyən etməklə və sonra onları daha spesifik elementlərə bölmək yolu ilə istifadə olunur. Şəbəkə infrastrukturunun layihələndirilməsinə sistemli şəkildə yanaşma prosesi, ümumi tələblərdən başlayaraq tədricən daha spesifik elementlərə bölünür. Bu prosesin hər bir mərhələsini daha ətraflı nəzərdən keçirək:

- Ümumi tələblərin müəyyənləşdirilməsi mərhələsində təşkilatın məqsəd və vəzifələrini, həmçinin proqram və xidmətləri dəstəkləmək üçün şəbəkə infrastrukturu tələblərini müəyyən edir.

- Tətbiqlərin və xidmətlərin inkişafı mərhələsində müəyyən edilmiş tələblərə əsasən, proqramlar və xidmətlər təşkilatda istifadə edilmək üçün dizayn edilir və hazırlanır.

- Tətbiq, təqdimat və seans səviyyələrinin müəyyən edilməsi mərhələsində istifadəçilərin interfeyslər, məlumatların təqdimatı və sessiyanın idarə edilməsi vasitəsilə tətbiqlərlə necə qarşılıqlı əlaqədə olduğunu müəyyən edən mühüm sistem komponentləri formalaşdırılır.

- Şəbəkə infrastrukturunun dizaynı mərhələsində tətbiqləri və xidmətləri dəstəkləyəcək şəbəkə infrastrukturu dizayn edilir. Bura şəbəkə cihazlarının, şəbəkə topologiyasının, protokollarının və texnologiyalarının seçimi daxildir.

- Təşkilatın tətbiqi və xidmət tələblərinə cavab verməsi mərhələsində şəbəkə infrastrukturunun layihələndirilməsi ilə bağlı bütün qərarlar performans, təhlükəsizlik, əlçatanlıq və miqyaslılıq kimi təşkilatın tətbiqi və xidmət tələblərinə cavab verməlidir.

Beləliklə, şəbəkə infrastrukturunun layihələndirilməsi zamanı səmərəli ötürülmə və emalın təmin edilməsi üçün məlumatların xüsusiyyətləri, trafik növləri və tələb olunan xidmətlərin xüsusiyyətləri nəzərə alınmalıdır.

Aşağıdan yuxarıya sistem yanaşması ayrı-ayrı komponentlərin və ya alt sistemlərin təhlili ilə başlayır və sonra onları daha böyük sistemlərə inteqrasiya edir. Bu yanaşma mövcud sistemləri optimallaşdırarkən və təkmilləşdirərkən və ya mürəkkəb şəbəkə strukturlarını təhlil edərkən faydalı ola bilər. Bu məqsədlərə çatdıqdan sonra şəbəkə data mərkəzi, server, filial, giriş nöqtəsi, paylama və əsas səviyyə, internet bağlantısı daxil olmaqla modullaşdırılmalıdır.

Modul tətbiqini reallaşdırmaq üçün məntiqi toplogiyadan istifadə olunur. Məntiqi topologiya komponentlərin fiziki təşkilindən asılı olmayaraq şəbəkədəki qurğular arasında məlumatların ötürülmə üsulunu müəyyən edir. O, marşrutlar, protokollar və trafikin idarə edilməsi daxil olmaqla, məlumatların şəbəkə vasitəsilə göndəricidən qəbulediciyə keçdiyi yolu təsvir edir. Məntiqi topologiya məlumatların şəbəkə vasitəsilə göndəricidən alıcıya keçdiyi marşrutları müəyyən edir.

Fiziki topologiya ilə məntiqi topologiyanın fərqli cəhətləri cədvəl 3.1-də təsvir olunmuşdur. Həmçinin şəbəkədəki cihazlar arasında məlumat ötürmək üçün istifadə olunan keçid protokollarının növlərini müəyyən edir. Məsələn, Ethernet, Wi-Fi, ATM (Asynchronous Transfer Mode) və digər protokollar xüsusi şəbəkə konfiqurasiyasından asılı olaraq məlumatların ötürülməsi üçün istifadə edilə bilər. Məntiqi topologiyaya prioritetləri, marşrutlaşdırmanı və xidmət keyfiyyətini müəyyən etməklə şəbəkədə məlumat axınını tənzimləyən trafikin idarə edilməsi daxildir. Bu, şəbəkə performansını optimallaşdırmağa və şəbəkə resurslarından səmərəli istifadəni təmin etməyə kömək edir. Məntiqi şəbəkə topologiyası verilənlərin şəbəkə üzrə necə hərəkət etdiyini müəyyən

etməkdə əsas rol oynayır və şəbəkənin təşkilatın tələblərinə və məqsədlərinə uyğun olaraq səmərəli işləməsini təmin edir. Əvvəldə qeyd etdiyimiz kimi, fiziki topologiyanın Nöqtədən-Nöqtəyə (Point to Point), Tor (Mesh), Ulduz (Star), Şin (Bus), Ring (Halqa), Ağac (Tree), Hibrid (Hybrid) növləri mövcuddur.

Fiziki topologiya ilə məntiqi topologiyanın fərqli cəhətləri

Cədvəl 3.1.

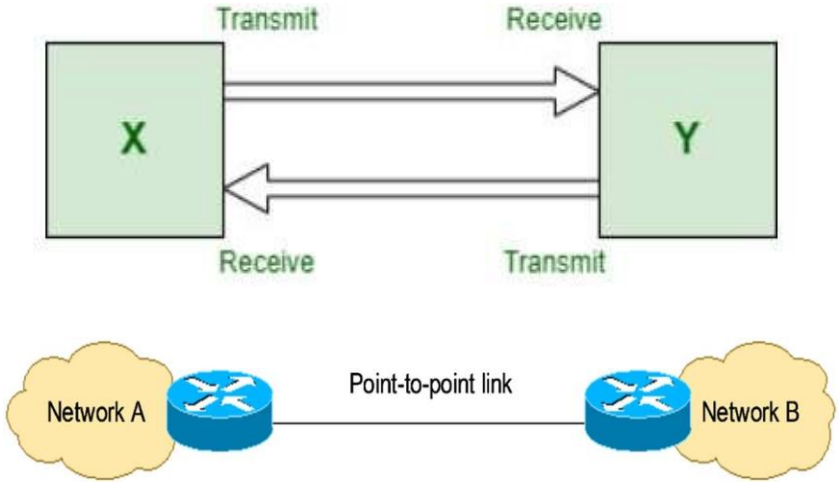
Fiziki topologiya	Məntiqi topologiya
Şəbəkənin fiziki quruluşunu göstərir.	Məlumat ötürülməsi ilə əlaqəli şəbəkə logistikasını təsvir edir.
Tələblərdən asılı olaraq tərtibat dəyişdirilə bilər.	Burada heç bir müdaxilə və ya manipulyasiya yoxdur.
Bu, cihazların seçimindən və mövcudluğundan asılı olaraq qiymətə, genişlənmə qabiliyyətinə və şəbəkə ötürmə qabiliyyətinə əhəmiyyətli dərəcədə təsir göstərir.	Bu, məlumat paketlərinin sürətinə və çatdırılmasına əhəmiyyətli dərəcədə təsir göstərir. O, həmçinin məlumat axınını və məlumat paketlərinin nizamlı çatdırılmasını idarə edir.
Bu, əsl ötürmə yoludur.	Bu, məlumat axınının yüksək səviyyəli görünüşüdür.
Şəbəkənin fiziki əlaqəsidir.	Şəbəkəni izləyən məlumat yoludur.

Nöqtədən-nöqtəyə (Point to Point) topologiya[24]. Nöqtədən-nöqtəyə topologiyası iki cihazın bir-birinə birbaşa qoşulduğu fiziki şəbəkə topologiyasının sadə formasıdır (şəkil 3.4). Bu topologiyada iki cihaz arasında birbaşa əlaqə və konfiqurasiya asanlığını təmin edən yalnız bir yol mövcuddur. Bu topologiya şəbəkə təşkilinin ən sadə formalarından biridir. Trafiki idarə etmək üçün əlavə avadanlıq quraşdırmaq və ya şəbəkə açarlarını və ya marşrutlaşdırıcıları konfiqurasiya etməyə ehtiyac yoxdur. İki cihaz arasında yalnız bir birbaşa əlaqə olduğundan, Nöqtədən-nöqtəyə topologiyası yüksək ötürmə qabiliyyəti və etibarlı məlumat ötürülməsini təmin edir. Bir cihazın nasazlığı digərinin işinə təsir göstərmir.

Nöqtədən-nöqtə topologiyası kompüterləri modem vasitəsilə şəbəkəyə qoşmaq, VPN (Virtual Şəxsi Şəbəkə) qurmaq üçün marşrutlaşdırıcıları

[24] https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

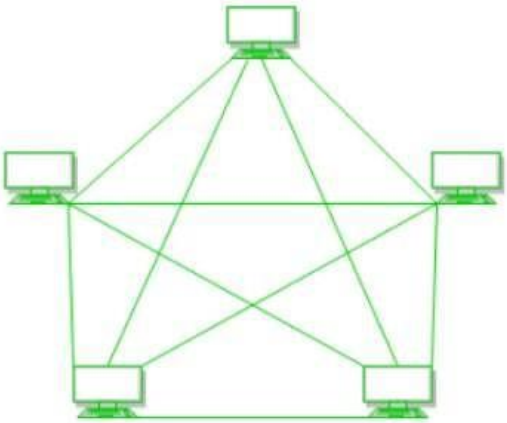
birləşdirmək və ya birbaşa iki LAN birləşdirmək kimi müxtəlif ssenarilərdən geniş istifadə olunur. Bununla belə, qeyd etmək lazımdır ki, Point-to-Point topologiyasının öz məhdudiyyətləri mövcuddur. O, digər topologiyalar kimi miqyaslı deyil və məsələn, ulduz və ya ağac topologiyaları kimi çox çeviklik və idarə olunmanı təmin etmir. O, həmçinin multi-hop bağlantılarını dəstəkləmir, bu da onu bir çox cihazı olan böyük şəbəkələr üçün yararsız edir.



Şəkil 3.4. Nöqtədən-nöqtəyə (Point to Point) topologiya

Tor (Mesh) topologiya. Mesh şəbəkə topologiyası, hər bir cihazın şəbəkədəki hər bir digər cihazla birbaşa əlaqəsi olan fiziki topologiyanın bir növüdür (şəkil 3.5).

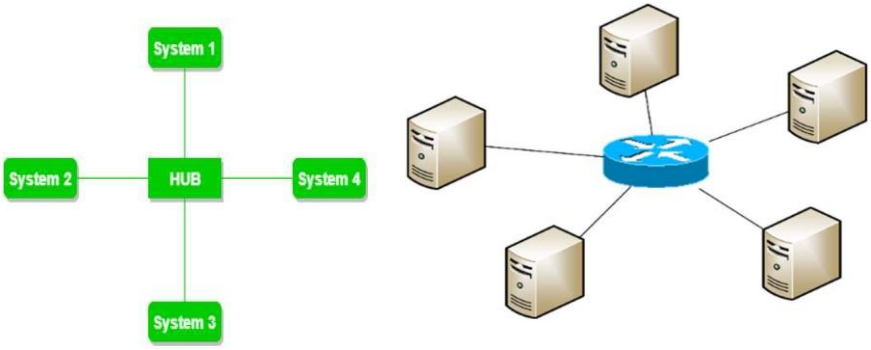
Bu toplogiyada, hər bir qovşaq digər qovşaqlarla bir neçə birbaşa əlaqəyə malikdir ki, bu da yüksək nasazlığa dözümlülüyünü və şəbəkənin etibarlılığını təmin edir. Mesh topologiyasının əsas məqsədi yüksək ötürmə qabiliyyəti və nasazlığa dözümlülüyü təmin etməkdir. Hər bir qovşağın digər qovşaqlarla çoxlu əlaqəsi olduğundan, bir əlaqənin uğursuzluğu rabitənin tam itməsi ilə nəticələnmir. Mesh şəbəkəsinin iş prinsipi ondan ibarətdir ki, verilənlər bir çox marşrutlar vasitəsilə göndəricidən alıcıya birbaşa ötürülə bilər. Bir marşrut qovşaq və ya kabel nasazlığı səbəbindən əlçatmazdırsa, məlumat digər mövcud marşrut vasitəsilə yönləndirilə bilər.



Şəkil 3.5. Tor (Mesh) topologiya

Bu, şəbəkənin etibarlılığını və nasazlıqlara dözümlülüyünü təmin edir. Bununla belə, Mesh şəbəkəsi daha çox əlaqə səbəbiylə ulduz və ya şin kimi digər topologiya növləri ilə müqayisədə daha çox resurs tələb edir. Buna görə də marşrutların sayının artması və məlumat ötürmə gecikmələri səbəbindən potensial performans problemləri nəzərə alınmalıdır. .

Ulduz (Star) topologiya. Ulduz şəbəkə topologiyası bütün cihazların keçid və ya mərkəz kimi mərkəzi qovşaqla birləşdirildiyi fiziki topologiyanın bir növüdür (şəkil 3.6).

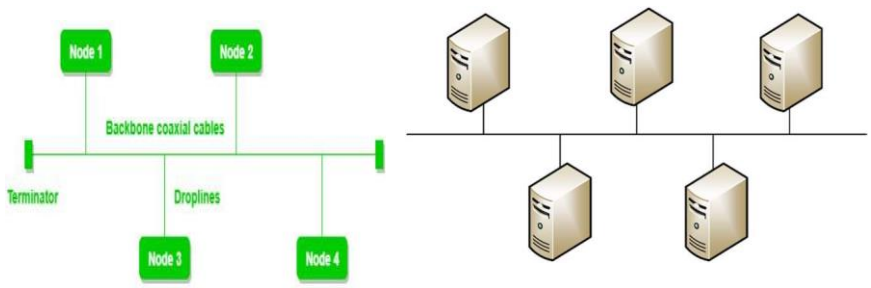


Şəkil 3.6. Ulduz (Star) topologiya

Bu topologiyada hər bir qurğunun mərkəzi qovşaqla ayrıca birbaşa əlaqəsi var ki, bu da idarəetmənin asanlığını və şəbəkənin yüksək etibarlılığını təmin edir. Ulduz topologiyasında bütün qurğular mərkəzləşdirilmiş idarəetmə nöqtəsi kimi çıxış edən mərkəzi qovşaqla əlaqələndirilir. Burada bütün

məlumatlar bir mərkəzdən paylandığı üçün şəbəkəyə nəzarəti, konfiqurasiyanı və idarə etməni asanlaşdırır. Ulduz topologiyasında yeni cihazları şəbəkəyə qoşmaq ağac və ya mesh kimi bəzi digər topologiyalara nisbətən daha asandır. Bu, ulduz topologiyasını kiçik və orta ölçülü təşkilatlar üçün cəlbedici seçimə çevirir. Ulduz topologiyasındakı bir cihaz uğursuz olarsa, şəbəkədəki digər cihazlar işlək vəziyyətdə qalarkən yalnız həmin cihaz əlaqəni itirir. Bu, ulduz topologiyasını halqa və ya şin kimi digər topologiyalardan daha etibarlı edir. Bununla belə qeyd etmək lazımdır ki, ulduz topologiyasındakı mərkəzi qovşaq tək uğursuzluq nöqtəsinə çevrilə bilər. Mərkəzi qovşaq uğursuz olarsa, ona qoşulmuş bütün qurğular şəbəkəyə girişi itirə bilər. Ulduz topologiyasının ötürmə qabiliyyəti mərkəzi qovşağın ötürmə qabiliyyətindən asılıdır. Əgər mərkəzi qovşaq yüksək ötürmə qabiliyyətinə malikdirsə, o zaman şəbəkə bütövlükdə yüksək ötürmə qabiliyyətinə malik olacaqdır. Ulduz topologiyası ev şəbəkələrində, kiçik ofislərdə və müəssisələrdə geniş istifadə olunan fiziki şəbəkə topologiyasının ən ümumi və sadə formalarından biridir. Asan idarəetmə və yüksək etibarlılığı təmin edir ki, bu da onu əksər şəbəkə mühitləri üçün seçimi cəlbedici edir.

Şin (Bus) topologiya. Şin topologiyası bütün cihazların şin adlanan bir mərkəzi kabelə qoşulduğu fiziki şəbəkə topologiyasının bir növüdür (şəkil 3.7).



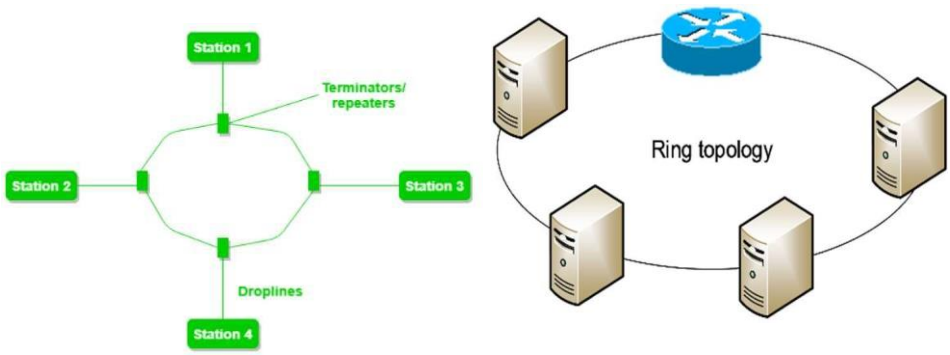
Şəkil 3.7. Şin (Bus) topologiya

Bu topologiyada hər bir cihaz giriş nöqtələri və ya birləşdiricilərdən istifadə edərək idarəetmə şininə qoşulur. Şin topologiyasında şəbəkədəki bütün cihazları birləşdirən yalnız bir kabel mövcuddur. Bu kabel bütün məlumatların cihazlar arasında ötürüldüyü şəbəkənin əsasını təşkil edir. Bu topologiya asan quraşdırmaya imkan verir, çünki bütün cihazları birləşdirmək üçün yalnız bir kabel tələb olunur. Bu onu kiçik şəbəkələr və ya ev şəbəkələri üçün cəlbedici

seçim edir. Şin topologiyası məhdud nasazlığa dözümlüdür. Mərkəzi kabel (şin)

uğursuz olarsa, bütün şəbəkə mövcud olmaya bilər. Bundan əlavə, bir cihazın və ya konnektorun uğursuzluğu bütün şəbəkəni poza bilər. Şin topologiyasının əsas çatışmazlıqlarından biri məlumatların toqquşması ehtimalıdır. İki cihaz eyni anda məlumat ötürməyə çalışdıqda, bu, şəbəkə performansını azaldan şin mübahisəsi ilə nəticələnə bilər. Şin topologiyasında şinin uzunluğu məhduddur və kabel nə qədər uzun olarsa, müdaxilə və siqnal itkisi ehtimalı bir o qədər çox olar. Şin topologiyası lokal şəbəkələrdə (LAN) istifadə edilən ilk topologiyalardan biridir. Xəta dözümlüyü və ötürmə qabiliyyəti məhdudiyyətlərinə görə indi yeni şəbəkələrdə nadir hallarda istifadə olunur, lakin yenə də kiçik şəbəkələrdə və ya laboratoriya mühitində cihazların bir-birinə qoşulması üçün istifadə edilə bilər.

Halqavari (Ring) topologiya. Halqa topologiyası fiziki şəbəkə topologiyasının bir növüdür, burada hər bir cihaz iki qonşu cihaza qoşularaq qapalı halqalı dövrə təşkil edir (şəkil 3.8). Bu topologiyada məlumat təyinatı üzrə çatana qədər halqa boyunca bir cihazdan digərinə ötürülür. Halqa topologiyasında hər bir cihaz qapalı halqa marşrutu yaradan iki qonşu cihaza qoşulur. Bu, cihazlar arasında məlumat ötürülməsi üçün qapalı bir marşrut təmin edir. Halqa topologiyasında hər bir cihaz öz qonşusuna məlumat ötürməklə mediaya bir-bir daxil olur. Bu, eyni vaxtda yalnız bir cihaz məlumat ötürə bildiyi üçün məlumatların qarşı durma və toqquşma ehtimalını azaldır.

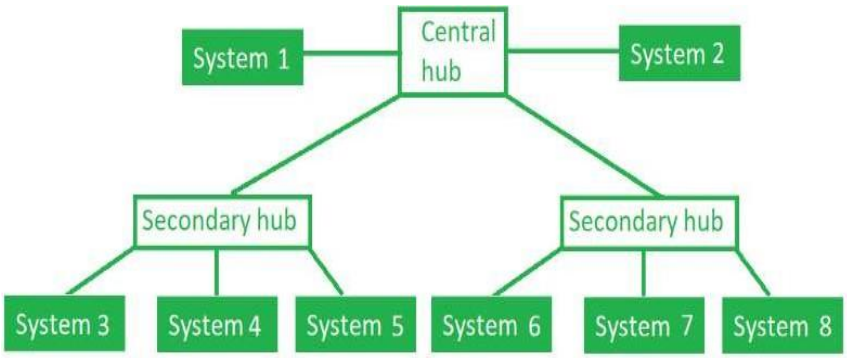


Şəkil 3.8. Halqavari (Ring) topologiya

Halqa topologiyası tam nasazlığa dözümlüdür. Bir uğursuz cihaz olarsa, halqada qurğular hələ də alternativ marşrut qalanlar vasitəsilə əlaqə saxlaya bilər. Bu, halqa topologiyasını şin topologiyaları kimi bəzi digər

topologiyalardan daha etibarlı edir. Halqa topologiyasında halqanın uzunluğuna görə ola bilər. Halqa nə qədər böyükdürsə və siqnal itkisi ehtimalı bir o qədər yüksəkdir. Halqanın uzunluğunu artırmaq üçün siqnal təkrarlayıcıları və ya gücləndiricilərdən istifadə edilə bilər. Halqa topologiyasında məlumat ötürülməsinə nəzarət etmək üçün halqa boyunca ötürülən işarədən istifadə mühitə girişi tənzimləyən Token Ring kimi xüsusi protokollardan istifadə edilə bilər. Ring topologiyası tez-tez yüksək nasazlığa dözümlülük və sabit məlumat ötürmə performansı tələb edən şəbəkələrdə istifadə olunur. Bununla belə, ya mesh kimi digər texnologiya və topologiyaların inkişafı, müasir şəbəkələrdə daha az rast gəlinir.

Ağacvari (Tree) topologiya. İyerarxik topologiya olaraq tanınan Ağac Topologiyası bir ağaca bənzər strukturda birləşdirilmiş bir neçə alt ağacın birləşməsidir (şəkil 3.9). Bu topologiyada digər alt ağacarın bağlandığı əsas alt ağac (adətən kök adlanır) mövcuddur.

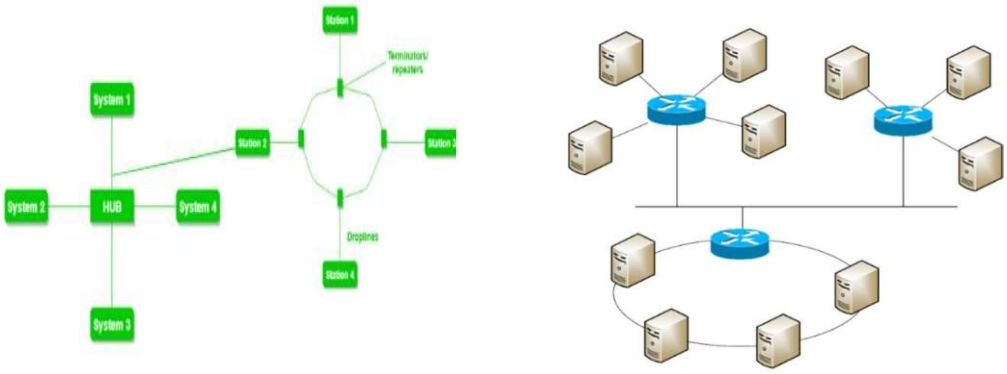


Şəkil 3.9. Ağac (Tree) topologiya

Ağac topologiyasında hər bir cihazın müəyyən səviyyədə olduğu iyerarxik quruluş var. İyerarxiyanın yuxarı hissəsində adətən mərkəzi marşrutlaşdırıcı və ya keçid rolunu oynayan kök cihaz yerləşir. Ağac topologiyası yüksək nasazlığa dözümlülük və çeviklik təmin edir. Bir cihaz uğursuz olarsa, bu, adətən şəbəkənin tam əlçatmazlığı ilə nəticələnmir, çünki uğursuz node-dan yan keçmək və alternativ yollarla məlumat ötürmək mümkündür. Mərkəzi cihaz, adətən kök cihaz, şəbəkənin idarə edilməsində mühüm rol oynayır. O, müxtəlif alt ağaclar arasında trafikə nəzarət edir və istiqamətləndirir, bütün şəbəkənin səmərəli idarə edilməsini və koordinasiyasını təmin edir. Ağac topologiyası korporativ şəbəkələr, təhsil müəssisələri və dövlət təşkilatları kimi

böyük şəbəkələrdə geniş istifadə olunur. O, yüksək səviyyəli nasazlıqlara dözümlülük və miqyaslılığı qoruyarkən səmərəli şəbəkə idarəetməsini və təşkilini təmin edir. Ağac topologiyası ulduz topologiyasının sadəliyi ilə şəbəkə topologiyasının çevikliyi arasında uzlaşmanı təmsil edir, şəbəkənin səmərəli idarə edilməsini və etibarlılığını təmin edir, eyni zamanda böyümə və genişlənmə üçün miqyaslılığı təmin edir.

Hibrid (Hybrid) topologiya. Hibrid topologiya iki və ya daha çox müxtəlif fiziki şəbəkə topologiyalarının birləşməsidir (şəkil 3.10).



Şəkil 3.10. Hibrid (Hybrid) topologiya

Bu, müxtəlif topologiyaların üstünlüklərini birləşdirməyə və təşkilatın xüsusi tələblərinə cavab verən daha çevik və adaptiv şəbəkə yaratmağa imkan verir. Hibrid topologiya istifadəçinin xüsusi ehtiyaclarına və şərtlərinə əsasən optimal şəbəkə dizaynını seçmək üçün çeviklik təmin edir. O, ulduz, halqa, ağac və ya mesh kimi müxtəlif topologiya növlərini vahid şəbəkə infrastrukturunda birləşdirməyə imkan verir. Hibrid topologiya, lazımsız marşrutlar və əlaqələrdən istifadə etməklə yüksək nasazlığa dözümlülük təmin edə bilər. Şəbəkənin bir hissəsi uğursuz olarsa, digər hissələr xidmətin davamlılığını təmin edərək işləməyə davam edə bilər. Müxtəlif növ topologiyaları birləşdirərək, şəbəkə performansını müxtəlif trafik növləri və tətbiqlər üçün optimallaşdırmaq olar. Məsələn, yüksək sürətli məlumat ötürülməsi üçün şəbəkə və ya halqa seqmentləri, cihazları birləşdirmək üçün ulduz və ya ağac topologiyaları istifadə edilə bilər.

Hibrid topologiya bütün şəbəkəni yenidən qurmadan yeni cihazlar əlavə etməyə və şəbəkə infrastrukturunu genişləndirməyə imkan verən şəbəkə

miqyasını təmin edir. Bu, hibrid topologiyanı böyüyən təşkilatlar üçün ideal

seçim edir. Bununla belə, hibrid topologiyanı qurmaq və idarə etmək sadə topologiyalardan daha mürəkkəb ola bilər, çünki o, müxtəlif şəbəkə komponentlərinin əlaqələndirilməsini və onların qarşılıqlı əlaqəsini idarə etməyi tələb edir. Hibrid topologiya yüksək şəbəkə dayanıqlığı, çeviklik və genişlənmə qabiliyyəti tələb edən böyük təşkilatlar üçün məşhur seçimdir. O, səmərəli fəaliyyəti və xidmətin davamlılığını təmin etməklə yanaşı, şirkətin xüsusi ehtiyaclarına və biznes məqsədlərinə cavab verən şəbəkə yaratmağa imkan verir.

FİZİKİ BAĞLANTI PROBLEMLƏRİNİN ARADAN QALDIRILMASI

Şəbəkə konnektorları[25] bütün trafik axınının vacib hissəsidir, çünki onlar hər bir rabitə əlaqəsinin başlanğıcı və sonudur. Bağlayıcılarla (S1) probleminiz varsa, hər bir yuxarı səviyyədə probleminiz olacaq və proqramlar işləməyəcək. Bağlayıcılar problemlərə həssasdır, çünki onlar tez-tez istifadə olunur və şəbəkə daxilində köçürülür. Bağlayıcıların bəzi hissələri, heç vaxt başlanğıc mövqeyindən tərpənməyən naqillər kimi digər şəbəkə komponentlərindən fərqli olaraq, onlardan istifadə zamanı nasaz ola bilər. Çox sayda bağlayıcı növlərini alaraq, birləşdiricinin uğursuz ola biləcəyi bir çox fərqli yol mövcuddur. Konnektoru (məsələn, RJ45 Ethernet konnektoru) təhlil edərkən aşağıdakı aspektləri diqqətlə yoxlamalısınız:

- Naqillərin sırası da daxil olmaqla, düzgün sarılmış olduğunu yoxlayın.
- Bütün naqillərin metal birləşdirici bıçaqlara toxunduğunu və qıvrımın qismən olmadığını yoxlayın.
- Heç bir naqilin əskik olmadığını yoxlayın.
- Plastik kabel gödəkçəsinin bağlayıcıya bərkidilməsini yoxlayın (yəni, məftillər birləşdiricidən asılmayıb).
- RJ45 kilidinin konnektorda işlədiyini yoxlayın (əks halda konnektor portdan çıxacaq).

Yuxarıda qeyd olunan problemlərdən hər hansı biri varsa, S1 problemlərinin qarşısını almaq üçün konnektoru dəyişdirməyi düşünməlisiniz.

Qısa və açıq dövrələrdə nasazlıqların aradan qaldırılması. Ümumi naqil problemləri adətən qısa dövrə adlanır. Bununla belə, kabel problemləri həm

[25] https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

qısa dövrələri, həm də açıq dövrələri əhatə edir, bunlar tamamilə əks problemlərdir. Qısa qapanma, bir kabel və ya birləşdirici içərisində bir-birinə toxunan iki naqili əhatə edir. Normal iş rejimində bu baş verməməlidir, çünki kabeldəki hər bir naqil müstəqil siqnal ötürdüyü üçün digər naqillərlə qarşılıqlı əlaqənin qarşısını almaq üçün izolyasiya olunmuş qoruyucu içərisində təcrid olunur. İki naqil bir-birinə toxunarsa, onların hər biri ilə əlaqəli siqnallar birindən digərinə keçərək siqnal çatışmazlığına səbəb olur. Digər tərəfdən, açıq dövrə bir telin tamamilə kəsilməsini nəzərdə tutur. Bunu müəyyən etmək qısa qapanmadan daha asan ola bilər, çünki kəsilmiş kabelləri yoxlamaq daha asandır. Qısa qapanmada olduğu kimi, açıq dövrə də xüsusi tel/kabeldə əlaqə çatışmazlığı yaradır.

Qeyd: Bəzən qısa və ya açıq dövrə kiçik miqyasda yalnız aralıq əlaqə çatışmazlığına səbəb olur. Bununla belə, bu məsələlərdən birinin siqnalın deqradasiyasına səbəb olduğu bir vəziyyətlə qarşılaşmağınız ehtimalı azdır. Adətən bu ya daimi siqnal itkisi, ya da aralıq siqnal itkisidir.

Qısa və açıq dövrələrdə nasazlıqların aradan qaldırılması çətin ola bilər, çünki bu problemlər çox vaxt fiziki olaraq görünmür. Bəzən kabeli hərəkət etdirsəniz, siqnalın bərpasını görəcəksiniz və bu, sizi düzgün yola istiqamətləndirə bilər. Bununla belə, bu cür məsələlərin araşdırılması üçün tövsiyə olunan üsul mis və ya lifli kabellərlə işləyən kabel test etmə avadanlığından istifadə etməkdir (Şəkil 3.11).

Kabeli test etmə avadanlığı, dielektrik gücü, izolyasiya xüsusiyyətləri, xarici təsirlərə qarşı müqavimət və digər parametrlər kimi kabellərin müxtəlif xüsusiyyətlərini qiymətləndirmək üçün istifadə olunur. Bu cür avadanlıqların iş prinsipi aparılan yoxlamanın növündən asılıdır. Kabeli test etmə avadanlığının işləmə prnsipi aşağıdakı kimidir:

1. Elektrik gücünun (gərginliyin) testi – Kabel qırılmadan gərginliyə tab gətirmək qabiliyyətini yoxlamaq üçün yüksək gərginliyə məruz qalır. Tipik olaraq, kabel keçiricilərinə tətbiq olunan alternativ və ya birbaşa gərginlik yaradan yüksək gərginlikli generatorlar istifadə olunur. İzolyasiyanın pozulması baş verərsə, avadanlıq bu anı qeyd edir və sınaq uğursuz sayılır.

2. İzolyasiyanın dözümlülük testi – kabelin izolyasiya materialının cərəyan sızmasının nə dərəcədə effektiv qarşısını aldığını müəyyən etmək üçün onun müqavimətini qiymətləndirir. Bunun üçün kabelə müəyyən bir gərginlik tətbiq edilir və izolyasiyadan keçən sızma cərəyanı ölçülür.

3. Termal testi – kabel istiyə məruz qaldıqda xüsusiyyətlərini qorumaq qabiliyyətini yoxlamaq üçün müəyyən bir temperatura qədər qızdırılır. Bu, yüksək temperaturda izolyasiya materiallarının və keçiricilərin dayanıqlığını qiymətləndirməyə imkan verir.

4. Kabel uzunluğunun ölçülməsi və zədələnmənin müəyyən edilməsi – kabel uzunluğunu təyin etmək və nasazlıq yerlərini müəyyən etmək üçün reflektometriya üsullarından istifadə etməklə. Kabel boyunca bir impuls göndərilir və onun müxtəlif nöqtələrdən əks olunması təhlil edilir, bu da qüsurları aşkar etməyə imkan verir.

Şəkil 3.11. Kabel test avadanlığı

RJ45 kabelləri Ethernet vasitəsilə kompüterlər, marşrutlaşdırıcılar və açarlar kimi şəbəkə cihazlarını birləşdirmək üçün istifadə olunur. RJ45 kabelində naqillərin çəkilməsi üçün iki əsas standart var:

1. EIA/TIA 568A.
2. EIA/TIA 568B.

Hər iki standart RJ45 konnektoruna qoşulmaq üçün rəngli naqillərin kabel daxilində necə yerləşdirilməsini təsvir edir. Qeyd etmək lazımdır ki, hər iki standart eyni funksionallığı təmin edir və kabelin hər iki ucu eyni standarta bükülərsə və ya krossover istifadə edilərsə (bir ucu 568A, digəri 568B-ə bükülür) kabel düzgün işləyəcəkdir (cədvəl 3.2 və cədvəl 3.3).

Cədvəl 3.2.
EIA/TIA 568A standartı

Pin	Siqnal Adı	Təsvir	Kabel teli rəngi	Ad	Pin
1	TX+_D1	Məlumatların ötürülməsi+	Yaşıl zolaqlı ağ 	TX+_D1	1
2	TX-_D1	Məlumat ötürmək -	Ağ zolaqlı yaşıl və ya bərk yaşıl 	TX-_D1	2
3	RX+_D2	Data+ qəbul edin	Narıncı zolaqlı ağ 	RX+_D2	3
4	BI+_D3	İki istiqamətli+	Ağ zolaqlı mavi və ya tünd mavi 	BI+_D3	4
5	BI-_D3	iki istiqamətli-	Mavi zolaqlı ağ 	BI-_D3	5
6	RX-_D2	Məlumat almaq -	Ağ zolaqlı narıncı və ya bərk narıncı 	RX-_D2	6
7	BI+_D4	İki istiqamətli+	Qəhvəyi zolaqlı ağ 	BI+_D4	7
8	BI-_D4	iki istiqamətli-	Ağ zolaqlı qəhvəyi və ya bərk qəhvəyi 	BI-_D4	8

EIA/TIA 568A standartına uyğun olaraq kabel qoşulma diaqramı:
Yaşıl zolaqlı ağ (Ağ/Yaşıl) - Pin 1
Yaşıl - Pin 2
Narıncı zolaqlı ağ (Ağ/narıncı) - Pin 3
Mavi - Pin 4

Mavi zolaqlı ağ (Ağ/Mavi) - Pin 5
Narıncı - Pin 6
Qəhvəyi zolaqlı ağ (Ağ/Qəhvəyi) - Pin 7
Qəhvəyi - Pin 8
EIA/TIA 568B standartına uyğun olaraq kabel qoşulma diaqramı:
Narıncı zolaqlı ağ (Ağ/narıncı) - Pin 1
Narıncı - Sancaq 2
Yaşıl zolaqlı ağ (Ağ/Yaşıl) - Pin 3
Mavi - Pin 4
Mavi zolaqlı ağ (Ağ/Mavi) - Pin 5
Yaşıl - Pin 6
Qəhvəyi zolaqlı ağ (Ağ/Qəhvəyi) - Pin 7
Qəhvəyi - Pin 8
Standartlar arasındakı fərqlər:
EIA/TIA 568A: Ağ/Yaşıl/Yaşıl cütlər 1 və 2-ci sancaqlarda yerləşir.
EIA/TIA 568B: Ağ/narıncı/narıncı cütləri 1 və 2-ci sancaqlarda yerləşir.
Əks halda, tellərin düzülüşü demək olar ki, eynidır, yeganə fərq tel cütlərinin sırasındadır. Seçdiyiniz standart seçiminizdən və ya layihə tələblərinizdən asılıdır, lakin hər ikisi eyni işləyir.

Cədvəl3.3.
EIA/TIA 568B standartı

Pin	Siqnal Adı	Təsvir	Kabel teli rəngi	Ad	Pin
1	TX+_D1	Məlumatların ötürülməsi+	Narıncı zolaqlı ağ 	TX+_D1	1
2	TX-_D1	Məlumat ötürmək -	Ağ zolaqlı narıncı və ya bərk narıncı 	TX-_D1	2
3	RX+_D2	Data+ qəbul edin	Yaşıl zolaqlı ağ 	RX+_D2	3
4	BI+_D3	İki istiqamətli+	Ağ zolaqlı mavi və ya tünd mavi 	BI+_D3	4

5	BI-_D3	iki istiqamətli-	Mavi zolaqlı ağ 	BI-_D3	5
6	RX-_D2	Məlumat almaq -	Ağ zolaqlı və ya bərk yaşıl 	RX-_D2	6
7	BI+_D4	İki istiqamətli+	Qəhvəyi zolaqlı ağ 	BI+_D4	7
8	BI-_D4	iki istiqamətli-	Ağ zolaqlı qəhvəyi və ya bərk qəhvəyi 	BI-_D4	8

Siqnal (dB) itkisi ilə bağlı problemlərin aradan qaldırılması. Siqnal itkisi həm mis, həm də fiber kabel infrastrukturunda problemdir. Bu, göndərilən ilkin ötürmə əsasında təyinat yerində itirilmiş siqnalın faizi ilə təmsil olunur. Başqa sözlə, alınan siqnal göndərilən siqnal qədər güclü deyil. Siqnal itkisi də zəifləmə adlanır və siqnal media vasitəsilə getdikcə artır, bunlara aşağıdakılar daxildir:

- Mis (elektrik siqnalları).
- Fiber (işıq şüaları).
- Simsiz (radio dalğaları).
- Siqnal itkisinin miqdarı bir sıra müxtəlif meyarlardan asılıdır:
- Məsafə
- Son bağlayıcılar
- Kabel keyfiyyəti
- Son nöqtələr arasındakı yamalar
- Elektrik müdaxiləsi (mis kabellər üçün)
- Radio müdaxiləsi (simsiz trafik üçün)
- Siqnalın dəyişdirilməsi iki şəkildə ifadə edilə bilər:
- Siqnal qazancı: alınan siqnal ötürülən siqnaldan yüksəkdir.
- Siqnal itkisi: qəbul edilən siqnal ötürülən siqnaldan aşağıdır.

Siqnal itkisi loqarifmik miqyasdan istifadə etməyi əhatə edir. Bu loqarifmik davranış siqnalın deqradasiyasının dB sayına əsaslanan xətti miqyasda getməməsi deməkdir; əvəzinə, daha sürətli artır. Bunu misal

göstərmək üçün aşağıdakı misallardan istifadə edək: Əgər orijinal siqnal ilə qəbul edilən siqnal arasında itirilmiş 3dB fərq varsa, bu o deməkdir ki, qəbul edilən siqnal ötürülən siqnalın yarısıdır. Əgər fərq 10dB olarsa, bu o deməkdir ki, siqnal 20 dəfə pisləşib. 20dB-də siqnal itkisində 100 dəfə, 30dB-də isə siqnal itkisində 1000 dəfə fərq var.

Optik liflər vəziyyətində, onları uzun məsafələrə quraşdırarkən, siqnal itkisinin dərəcəsini tapmaq üçün MMF və ya SMF kabel xüsusiyyətlərini təhlil etməlisiniz. Məsələn, kabel istehsalçısı tərəfindən göstərilən siqnal itkisi hər km üçün 3dB ola bilər. Üstəlik, istehsalçı tərəfindən müəyyən edilmiş, adətən 1dB-dən (məsələn, 0.3dB) aşağı olan yamaq panellərinə siqnal itkisini əlavə etməlisiniz. Hər dəfə patch paneldən keçdiyiniz zaman siqnal gücünü itirirsiniz, beləliklə, 2 km məsafəni qət edən və iki patç paneldən keçən fiber kabel, əvvəllər qeyd olunan rəqəmlərə əsasən 6,6 dB uçdan uca siqnal itkisinə malikdir (hər 2x3 dB). km və hər patch panel üçün 2×0,3dB).

Siqnalın ilkin gücündən və qəbuledici son tələblərdən (məsələn, tətbiqlər, xidmətlər və s.) asılı olaraq, uzaq məsafələrdə dəqiq siqnal itkisini hesablamaq üçün diqqətlə təhlil aparılmalıdır.

TX/RX ilə bağlı problemlərin aradan qaldırılması. Kabel probleminin xüsusi bir növü, kabelin ötürücü və qəbuledici cütlərinin tərsinə çevrildiyi və beləliklə TX tərəflərinin bir-birinə və RX tərəflərinin bir-birinə bağlandığı bir problemdir (TX-ni düzgün birləşdirmək üsulundan fərqli olaraq) RX-ə). Ethernet mühitində bu, birbaşa kabelin krossover kabelə çevrilməsinə və əksinə ola bilər. Bu ssenarini müəyyən etmək asandır və cihazlar bunu avtomatik aşkar edib düzəldə bilsə, problem olmaya bilər. Bu funksionallıq avtomatik algılama və ya avtomatik MDIX adlanır və istifadəçi üçün şəffafdır. Xəta konnektorda və ya yamaq panelində bir yerdə ola bilər və bu, adətən insan səhvidir. Xəta kabelin içərisində olmadığı üçün, kabel sonlarını vizual olaraq təhlil etməklə onu müəyyən etmək nisbətən asan ola bilər. Bu tip problemlər fiber optik qurğularda da mövcuddur və iki formada ola bilər:

- Kabeldə cihazın yanlış portlarına daxil edilmiş xüsusi TX və RX konnektorları var.

- Kabelin tək konnektoru var (həm TX, həm də RX lifləri ilə) o, səhv bükülmüşdür (kabelin bir tərəfində TX kabelin digər tərəfində RX-ə).

- TX/RX problemlərini həll etmək üçün həll yollarına aşağıdakılar daxildir:

- Bağlayıcının dəyişdirilməsi.

- Yamaq panelinin sonunun dəyişdirilməsi.

- RX və TX konnektorlarının tərsinə çevrilməsi (yəni, optik liflər).

Digər növ kabel problemlərində olduğu kimi, dəqiq problemi və yeri tapmaq üçün siz kabel və birləşdirici konfiqurasiyalarda dəqiq nəticələr verə bilən xüsusi diaqnostika avadanlığından (məsələn, tel xəritəçəkmə cihazları) istifadə edə bilərsiniz.

Kabelin yerləşdirilməsi. Server şkafında səliqəli kabel marşrutu İT avadanlıqlarına texniki xidmətin asanlığını təmin etmək və server kabinetinizə peşəkar görünüş vermək üçün xüsusilə vacibdir. Bir çox təşkilatlar çoxlu sayda kabellərə xidmət göstərməkdə çətinliklərlə üzləşirlər, xüsusən də onlar etiketlənməmiş və hamısı eyni rəngdədirsə. Rəfinizi quraşdırmağa və təşkil etməyə başlamazdan əvvəl kabel idarəçiliyinizi əvvəlcədən planlaşdırmağınız tövsiyə olunur.

Kabel planlaşdırma strategiyası kabellərin haradan gəldiklərindən və hara getdiklərindən asılı olaraq dəyişə bilər. Bu, adətən kabellərin yuxarıdan, aşağıdan daxil olacağı və ya rafın içərisinə qoşulacağı deməkdir. Yamaq paneliniz varsa, tavandan keçən qalın kabelləri idarə etmək problemi ilə qarşılaşa bilərsiniz. Çözüm, xüsusi döngələrdən istifadə edərək bir panelə qoşulmuş bütün kabelləri bağlamaq və sonra yamaq kabellərini üfüqi kabel təşkilatçısı vasitəsilə keçirmək ola bilər (şəkil 3.12).

Şəkil 3.12. Kabel planlaşdırma strategiyası

Kabelləri rafın içərisinə birləşdirərkən, sadəcə kabelləri kabel kanalının kənarları boyunca keçirə və onları bərkidmək üçün zip bağlarından istifadə edə bilərsiniz. Hər halda, əsas fikir bir yerə yönəldilmiş kabelləri birləşdirmək və asanlıqla əldə edilə bilən kabel qrupunu rəf daxilində yığcam saxlamaqdır. Server şkafında kabellərin yönləndirilməsi üçün əsas aksesuarlar şaquli kabel idarəetmə çubuğu (şaquli kabel təşkilatçısı) hesab olunur. Bir çox raflar artıq onlarla birlikdə gəlir, lakin sizdə yoxdursa, uyğun bir seçim tapmağa çalışın. Bu çubuqlar istifadəçiyə siqnal və güc keçiricilərinin quraşdırılmasında daha çox çeviklik verir, onlar adətən naqilləri tutmaq üçün daxili qarmaqlar və ilgəklərə malikdirlər, lakin bəzən çevik borular kimi də mövcuddur. Əsasən, bütün kabellər bu şüaların içərisində yuxarı və ya aşağı çəkiləcəkdir. Şaquli kabel menecerləri nisbətən ucuzdur - çox güman ki, bütün şkafınız və ya rafınız üçün birinə ehtiyacınız olacaq (şəkil 3.13).

Şəkil 3.13. Şaquli kabel menecerləri

Şəbəkə avadanlığını ön tərəfdən və yamaq panellərinə birləşdirərkən, yüngül və istifadəsi asan olan D-halqalı çubuqlar və ya "daraqlar" kimi xüsusi üfüqi kabel idarəçilərinə malik olmaq lazımdır. Kabelləri daha zərif şəkildə təşkil etmək üçün qapaqlı kabel menecerlərindən də istifadə edə bilərsiniz. Şaquli kabel təşkilatçıları bir rafın içərisində istifadə olunursa və onlarla kabeli bir qalın dəstəyə yığmaq üçün xidmət edirsə, üfüqi olanlar kabelləri kabinetdən kənarda, ümumiyyətlə ön tərəfdə bərabər paylamaq üçün istifadə olunduğunu başa düşmək vacibdir. Onların əsas vəzifəsi kabellərin ağırlığını götürmək,

yararsız "dolamaları" çıxarmaq və ya bağlayıcıları təsadüfən çəkilməkdən qorumaqdır (şəkil 3.14).

Şəkil 3.14. Yamaq panel

Bağlama və ya sıxaclar (xomut) – bu kiçik məhsullar çox yönlüliyi ilə avtomobil və elektrik sahələrində ən çox yayılmışdır, lakin gündəlik həyatda da istifadə olunur (şəkil3.15). Lakin onların istifadəsi müəyyən çətinliklər yaradır. Birincisi, kabel bağları kabeli həddindən artıq sıxa bilər, bu da onun daxili keçiricilərinə zərər verə bilər. İkincisi, sıxacların bərkidilməsini tənzimləmək qabiliyyəti yoxdur, bu da kabelin qeyri-bərabər bərkidilməsinə səbəb ola bilər və sıxacın sıxılmasına baxmayaraq, onu boşalta bilməyəcəksiniz. Üçüncüsü, zaman keçdikcə və ultrabənövşəyi işığın və ya havanın təsiri altında bağlar partladı.

Şəkil 3.15. Bağlama və ya sıxaclar (xomut)

Kabelin quraşdırılması, çarpaz əlaqənin və ya digər problemlərin uç-uca rabitəyə təsir etmədiyinə əmin olmaq üçün istehsala başlamazdan əvvəl diqqətlə sınaqdan keçirilməlidir. Bu proses zamanı xüsusi sınaq avadanlığı tövsiyə olunur.

ETHERNET STANDARTLARI

Ethernet[26] geniş yayılmış texnologiyadır və şəbəkə dünyasında istinaddır. İstifadə olunan media növündən (məsələn, mis, fiber və ya simsiz) və sürətdən (10Mbps, 100Mbps, 1Gbps və ya 10Gbps) asılı olaraq bir çox əlaqəli standartlara malikdir. Köhnə Ethernet standartları koaksial kabelə əsaslanırdı, lakin müasir şəbəkələrdə belə deyil. Ən vacib Ethernet standartları aşağıdakılardır: 10BaseT, 100BaseT, 1000BaseT, 100BaseTX, 100BaseFX, 1000BaseX, 10 GBaseSR, 10GBaseLR, 10GBaseER, 10GBaseSW, 10GBazLW, 10GBazEW, 10GbaseT.

Bu standartların adlandırma konvensiyasına baxarkən nümunə görə bilərsiniz. Birinci hissə standartın işlədiyi maksimum sürəti aşağıdakı kimi müəyyənləşdirir:

10 = 10 Mbps
100 = 100Mbps
1000 = 1Gbps
10G = 10Gbps

“Base” baza diapazonu deməkdir, yəni kabellər məlumatları bir ucundan digərinə göndərmək üçün bir tezlikdən istifadə edir. Əsas zolaqlı texnologiyadan fərqli olaraq, Genişzolaqlı texnologiya ortaq bir mühit (məsələn, TV kabelləri) üzərində işlədiyi üçün məlumat göndərmək üçün bir çox tezliklərdən istifadə edir. Adlandırma konvensiyasının sonuncu hissəsi mis (T bükülmüş cütdən gəlir) və ya fiber optik (digər qısaltmalar) ola bilən standart tərəfindən istifadə olunan media növünü müəyyən edir.

10BaseT. 10BaseT Ethernet-in əvvəlki bükülmüş cüt standartlarından biridir və maksimum 10Mbps ötürmə qabiliyyəti təklif edir. T bükülmüş cütü

[26] Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.
Шаньгин В.Ф. Защита информации в компьютерных системах и сетях М.: ДМК Пресс, 2012. 592 с.

təmsil edir (yəni, mis əsaslı standartdır). Bu standart standart UTP kabelində mövcud olan dörd cütdən yalnız iki cütdən istifadə edir (bir cüt Ötürmə, digəri Qəbul üçün). 10BaseT ilk dəfə təqdim edildikdə, istifadə edilən standart kabel maksimum 100 m məsafədə işləyən 3-cü kateqoriyalı kabel idi.

100BaseT. 10Mbps şəbəkə istifadəçilərinin artan ehtiyGNSarı üçün kifayət etmədiyindən, FastEthernet kimi də tanınan 100BaseT standartı hazırlanmışdır. 100BaseT-in daha yüksək sürətləri kabel baxımından daha yüksək tələbləri də əhatə edir. Bu standart Kateqoriya 5 və ya daha yüksək olan burulmuş cüt mis kabeldən istifadə edir və maksimum 100 m məsafədə işləyir. Bu standart həmçinin standart UTP kabelində mövcud olan dörd cütdən yalnız iki cütdən istifadə edir (bir cüt Ötürmə, digəri isə Qəbul üçün).

100BaseFX. 100BaseFX 100BaseT-in ekvivalentidir, yeganə fərq odur ki, mis kabellər əvəzinə fiber bağlantılar üzərində işləyir. Cüt optik liflərdən biri Ötürmə məqsədləri üçün, digəri isə Qəbul məqsədləri üçün istifadə olunur, beləliklə tam dupleks funksiyasına nail olur. İki növ lif bağlantısı bu standartı dəstəkləyir:

1. Tək rejimli lif: 2 km-dən çox məsafədə işləyir.
2. Çox rejimli lif: maksimum 400 m (yarım dupleks) və ya 2 km (tam dupleks) məsafədə işləyir.

1000BaseT. Növbəti təbii addım 100Mbps-dən 1Gbps-ə qədər artım oldu, beləliklə, 1000BaseT standartı. Bu, həmçinin Kateqoriya 5 kabeli üzərində işləyir, lakin adətən Cat 5e və ya Cat 6 kabelləri ilə istifadə olunur. 100BaseT standartından fərqli olaraq, 1000BaseT UTP kabelində dörd şəbəkə cütünün hamısından istifadə edir.

1000BaseX. 1000BaseX, 1000BaseT-in fiber optik müxbiridir və istifadə olunan lifin növündən asılı olaraq bir çox variasiyada olur:

1000BaseSX: qısa dalğa uzunluğunda lazer (550 m-ə qədər)

1000BaseLX: uzun dalğa uzunluğunda lazer (5 km-dən çox)

10GBase Standartları. Məlumat mərkəzi şəbəkəsində istifadə olunan ən mühüm 10Gbps standartları bunlardır: 10 GBaseSR, 10GBaseLR, 10GBaseER

10GBaseSR (Qısa Range) standartı qısa məsafəli rabitədən istifadə etməklə işləyir. Əvvəlcə 80 m-ə qədər işlədi, lakin düzgün çox rejimli lifdən istifadə edərək 300 m-ə qədər gedə bilər. O, ümumiyyətlə bir otaqda və ya bir məlumat mərkəzinin içərisində istifadə olunur.

10GBaseLR (Long Range) daha uzun diapazonlarda işləyir və bu səbəbdən çox rejimli lif əvəzinə tək rejimli lifdən istifadə edir. Bu standart adətən 25 km-

ə qədər işləyir və yüksək güclü işıq siqnalının belə uzun məsafəni keçə bilməsini təmin etmək üçün lazerlərdən istifadə edir.

10GBaseER (Genişləndirilmiş Range) tək rejimli lifdən istifadə edərək daha böyük məsafələrdə işləyir. 40 km məsafə qət edə bilir.

WAN üzərindən 10G. Xidmət təminatçıları WAN üzərindən işləyən aşağıdakı 10G Ethernet standartlarından istifadə edə bilər: 10GBaseSW, 10GbazLW, 10GbazEW.

Bu standartlar 10GBaseSR/LR/ER standartlarına (adətən müəssisə məlumat mərkəzində istifadə olunur) uyğun gəlir və onlar qısa, uzun və geniş əməliyyat diapazonundan istifadə edirlər. Bu, eyni növ liflər və birləşdiricilərdən istifadə edərək SONET/SDH WAN ilə 10Gbps Ethernet bağlantısını birləşdirir və SR/LR/ER standartları ilə eyni məsafələrdə işləyir.

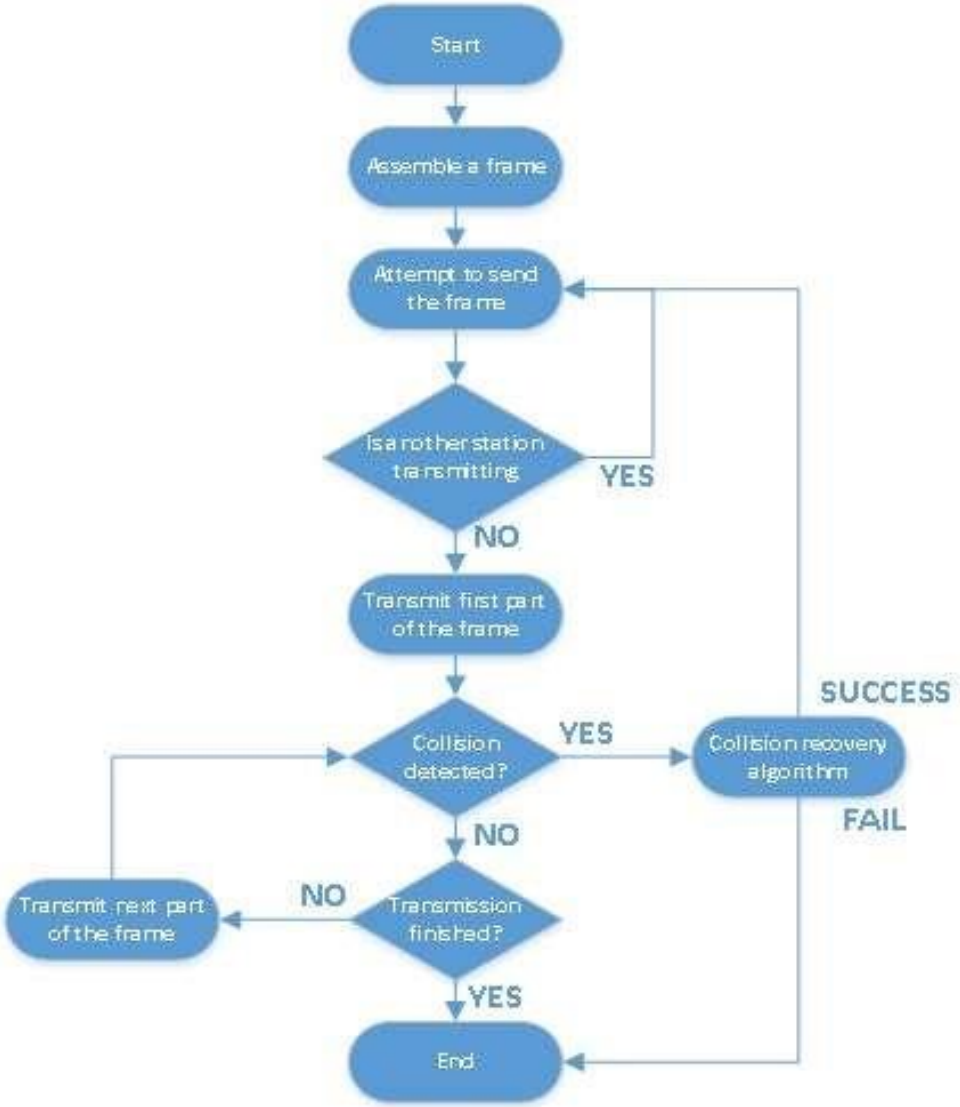
10GbaseT. 10GBaseT, optik liflərdən istifadə etmək istəmədiyiniz hallarda mis kabellər (burulmuş cüt) üzərindən 10Gbps ötürməyə imkan verən xüsusi standartdır. Bu standart aşağıdakı media növlərindən istifadə edir:

1. Kateqoriya 6 kabel – 55 m-ə qədər işləyir.
2. Kateqoriya 6a kabel – 100 m-ə qədər işləyir.

CSMA/CD. CSMA/CD və CSMA/CA şəbəkə dünyasında ümumi abbreviaturadır. CSMA-dakı CS Carrier Sense deməkdir və bu o deməkdir ki, şəbəkədə əlaqə saxlayan cihaz başqa bir stansiyanın mühitdə ötürmə olub olmadığını müəyyən etmək üçün dinləyir. Əgər belədirsə, o, artıq mövcud olan siqnal üzərindən ötürməyəcək. CSMA-da MA çoxlu giriş deməkdir və bu o deməkdir ki, şəbəkədə eyni vaxtda əlaqə qurmağa çalışan birdən çox cihaz var. CSMA/CD-dəki CD toqquşmanın aşkarlanması deməkdir. Ethernet toqquşması iki stansiya naqildə eyni vaxtda siqnal göndərdikdə və siqnallar toqquşduqda, şəbəkədə heç kim siqnalların heç birini başa düşə bilmədikdə baş verir.

Çərçivə yığıldıqdan sonra stansiya digər stansiyalar tərəfindən ötürülə bilən hər hansı bir siqnal üçün naqili dinləyəcək. Əgər belə bir siqnal aşkar edərsə, o, paketi göndərməyəcək, əksinə yenidən cəhd etməzdən əvvəl bir müddət gözləyəcək. Əgər heç bir siqnal yoxdursa, o, çərçivənin birinci hissəsini ötürəcək və toqquşma olub-olmadığını görmək üçün gözləyəcək. Əgər belə olarsa, bu toqquşmada iştirak edən bütün stansiyalar geri çəkiləcək və siqnalı təkrar ötürməzdən əvvəl təsadüfi bir müddət gözləyəcəklər. Əgər toqquşma aşkar edilmirsə, stansiya kadrın növbəti hissəsini göndərir və toqquşmaların olub olmadığını yenidən yoxlayır. Bu proses çərçivə tam ötürülənədək davam edir.

Şəkil 3.16-da təsvir edilən ssenari seqmentdəki bütün stansiyalar bir-birini eşitdikdə, yəni yarım dupleks mühitlərdə (hublarda) baş verir.

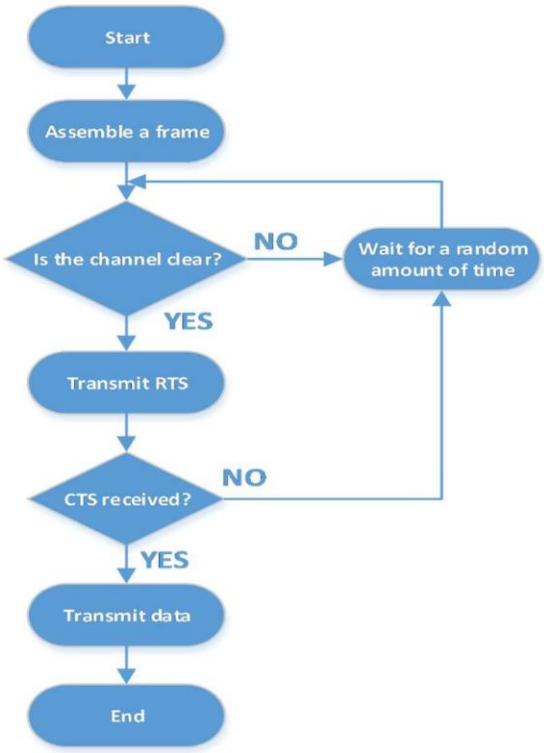


Şəkil 3.16. CSMA/CD üsulu

Yarım dupleks mühitlər stansiyalara müəyyən bir anda ötürməyə və ya qəbul etməyə imkan verir, lakin hər ikisini eyni anda deyil. CSMA/CD artıq geniş miqyasda istifadə edilmir, çünki müasir şəbəkələr hublar əvəzinə açarlardan istifadə edir. Açarlardan istifadə edərkən siz tam dupleks ötürmələrdən istifadə edə bilərsiniz, yəni siz eyni vaxtda həm göndərə, həm də qəbul edə bilərsiniz.

CSMA/CA. CSMA/CA ilə CA toqquşmadan qaçma deməkdir ki, bu da Toqquşmanın Aşkarlanmasından fərqli bir konsepsiyadır, çünki stansiyalar sadəcə onu aşkar etmək əvəzinə hər cür toqquşmadan qaçmağa çalışırlar. Bu, ümumiyyətlə simsiz şəbəkələrdə istifadə olunur, çünki simsiz cihaz müəyyən bir anda digər stansiyalar arasında əlaqənin olub-olmadığını eşidə bilmir (beləliklə, CD-dən istifadə edə bilməz). Belə bir mühitdə plan şəbəkədə məlumat göndərməzdən əvvəl hər hansı bir toqquşmanın qarşısını almaqdır və bu, adətən RTS/CTS (göndərməyə hazır/göndərməyə təmiz) kimi həyata keçirilir. Bu adətən simsiz şəbəkənin mərkəzi nöqtəsi - giriş nöqtəsi (AP) tərəfindən idarə olunur.

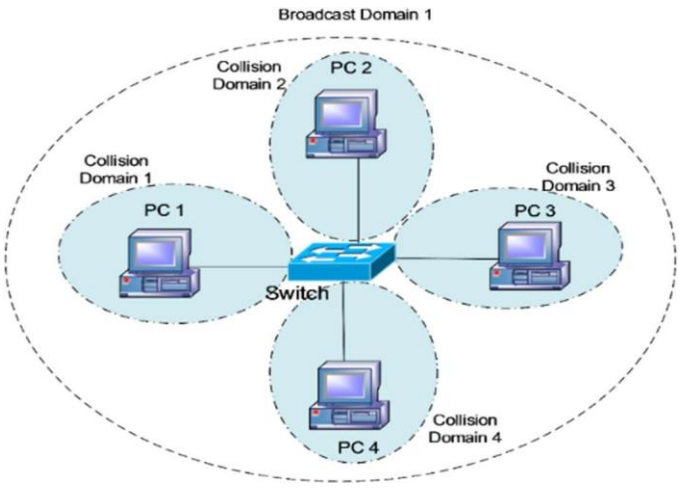
Stansiyalar trafik göndərməzdən əvvəl, AP əvvəlcə onlara bunu etmək üçün icazə verməlidir və həmin vaxt toqquşmaların qarşısını almaq üçün başqa heç bir trafikin olmadığını təsdiq etməlidir. Stansiya aydın siqnalı gözləməli olduğundan, AP müəyyən vaxtda yalnız bir stansiyanın trafik göndərdiyinə əmin ola bilər. Bu qərar prosesi şəkil 3.17-də təsvir edilmişdir.



Şəkil 3.17. CSMA/CA üsulu

Şəkildən göründüyü kimi, çərçivə yığıldıqdan sonra stansiya kanalın aydın olmasının təsdiqini gözləməli və yalnız bundan sonra məlumatları ötürə bilər. Əgər stansiyalar AP-dən CTS təsdiqini almazsa, onlar RTS sorğusunu yenidən göndərməzdən əvvəl təsadüfi vaxt gözləməlidirlər. Bu texnika həm də stansiyanın AP-ni görə bildiyi, lakin şəbəkənin digər tərəflərindən yalnız AP vasitəsilə əldə edilə bilən digər stansiyaları görə bilməməsi problemini də həll edir (yəni, AP mərkəzi nöqtə olduğu üçün hər stansiyaya çata bilər).

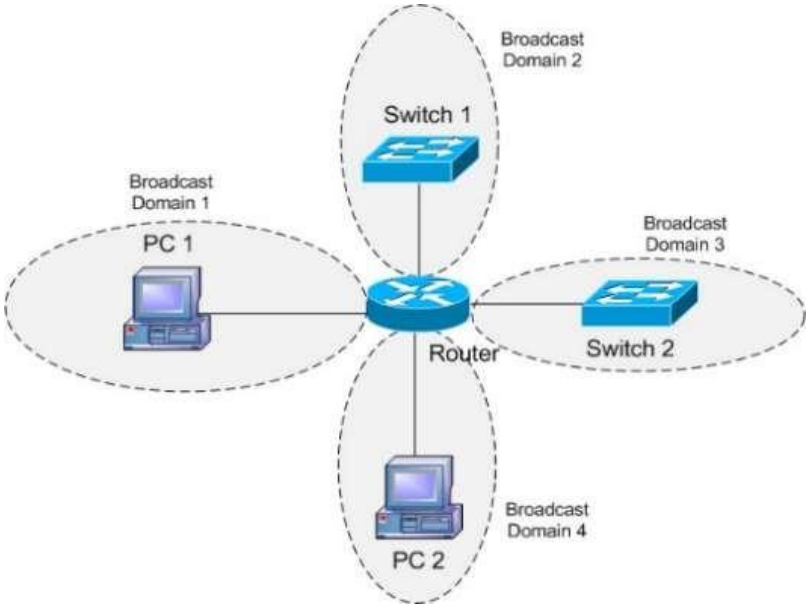
Toqquşma və yayım (Broadcast) domenləri. Bu kitabda daha əvvəl təsvir edildiyi kimi, şəbəkə hublarının əsas çatışmazlıqlarından biri naqildə toqquşma zamanı zədələnmiş çərçivənin bütün qoşulmuş cihazlara göndərilməsidir. Müasir kommutatorların üstünlüklərindən biri odur ki, keçiddəki hər bir port toqquşma domeni hesab olunur. Toqquşma halında (tam dupleks mühitlərdə bu mümkün deyil), zədələnmiş çərçivə interfeysdən keçmir. Kommutatorlar yayım domenlərini ayırmır, marşrutlaşdırıcılar ayırır. Əgər keçid Yayım təyinat ünvanı olan çərçivə qəbul edərsə, o zaman onu çərçivənin qəbul edildiyi portdan başqa bütün portlardan kənara yönləndirməlidir. Yenə də yayım domenlərini ayırmaq üçün marşrutlaşdırıcı tələb olunur. Şəkil 3.18-da toqquşma domenlərinin necə ayrıldığını göstərmək üçün açarlar/körpülər və marşrutlaşdırıcılardan istifadə edən kiçik şəbəkəni əks etdirir[27].



Şəkil 3.18. Toqquşma və yayım (Broadcast) domenləri

27 https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

Keçid portuna qoşulmuş cihazlar eyni toqquşma domenindədir, lakin müxtəlif portlara qoşulmuş cihazlar müxtəlif toqquşma domenlərindədir. Bu, keçidin ən vacib xüsusiyyətidir: o, toqquşma domenlərini ayırır. Şəkil 3.19-da Yayım (Broadcast) domenləri təsvir olunmuşdur.



Şəkil 3.19. Yayım domenləri

Routerlər defolt olaraq Multicast və Broadcast paketlərini bloklayır. Bu, marşrutlaşdırıcı və keçid arasındakı əhəmiyyətli fərqdir və şəbəkədə ötürmə qabiliyyəti istifadəsinə nəzarət etməyə kömək edir. Eyni marşrutlaşdırıcı portuna qoşulmuş cihazlar eyni toqquşma və yayım domenlərindədir, lakin müxtəlif marşrutlaşdırıcı portlarına qoşulan cihazlar fərqli toqquşma və yayım domenlərindədir.

NAQİLLƏRİN PAYLANMASI TEXNOLOGİYASI

Paylama çərçivələri (Distribution Frames)[28]. Paylayıcı çərçivə şəbəkənin passiv kabelin dayandırılması kimi çıxış edən fiziki hissəsidir. Bu, kabellərin delindiyi yerdir və o, yamaq panellərindən və zımbalı bloklardan ibarətdir.

[28] https://www.howtonetwork.com/comptia-network-study-guide-free/
https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

Paylama çərçivələri kabel sistemi üçün mərkəzi konsentratordur, məsələn, məlumat mərkəzindən gələn və istifadəçi bloklarına gedən kabellər və onlar bir neçə formada ola bilər:

1. Avtonom bloklar.
2. Manual bloklar.

Paylama çərçivələri də media növünə və məqsədinə görə bir neçə növdə ola bilər:

- Mis üçün paylama çərçivələri.
- Fiber üçün paylama çərçivələri.
- Məlumat üçün paylama çərçivələri.
- Səs üçün paylama çərçivələri.

Böyük mühitlərdə paylama çərçivələri şəbəkənin kritik hissəsi olduğu üçün xüsusi otaqda yerləşdirilir, çünki şəbəkədəki bütün məlumat axınları paylama çərçivələrindən keçir. Xüsusi siqnal növləri üçün paylama çərçivələrinin xüsusi adları var:

- Audio paylama çərçivəsi (APÇ).
- Rəqəmsal paylama çərçivəsi (RPÇ).
- Fiber optik paylama çərçivəsi (FOPÇ).
- Video paylama çərçivəsi (VPÇ).

Audio paylama çərçivəsi (APÇ) – telefon və ya radio şəbəkələri kimi şəbəkələr üzərində analoq və rəqəmsal səs siqnallarını yaymaq üçün istifadə olunur.

Rəqəmsal paylama çərçivəsi (RPÇ) – məlumat, səs və digər rəqəmsal axınları ötürmək üçün telekommunikasiya şəbəkələrində geniş istifadə olunan rəqəmsal siqnalları yaymaq üçün nəzərdə tutulmuşdur.

Fiber optik paylama çərçivəsi (FOPÇ) – fiber optik kabelləri idarə etmək və yaymaq üçün istifadə olunur. O, fiber-optik şəbəkələrdə optik siqnalların qoşulmasını və marşrutlaşdırılmasını təşkil etməyə imkan verir.

Video paylama sistemi (VPÇ): Bu çərçivə video siqnalları, məsələn, televiziya şəbəkələrində və ya video nəzarət sistemlərində yaymaq üçün istifadə olunur.

Bu çərçivələrin hər biri ötürmə keyfiyyətini yaxşılaşdıran və şəbəkə idarəetməsini asanlaşdıran xüsusi siqnal növü ilə işləmək üçün optimallaşdırılıb.

Demarkasiya nöqtələri. Demarkasiya nöqtələri daxili infrastrukturu xarici dünya ilə birləşdirən şəbəkə nöqtələridir. Onlar adətən şəbəkənin mərkəzində yerləşərək WAN və İnternet bağlantısı üçün istifadə olunur.

Demarkasiya nöqtələri təkcə müəssisə mühitlərində deyil, həm də kiçik şəbəkələrdə və ya hətta yaşayış yerlərində (məsələn, televizor, telefon və ISP-ni birləşdirən nöqtələr) mövcuddur. Müəssisə mühitlərində demarkasiya nöqtələri adətən əsas məlumat mərkəzində yerləşdirilir, çünki onların əsas şəbəkə cihazları ilə sıx əlaqəsi olmalıdır. Bu, RJ45 və ya WAN bağlantılarını birləşdirə bilən lif konnektorları olan sadə qutu kimi bir şey ola bilər.

Ağıllı jaklar (Smart Jacks). "Smart Jacks" (və ya "ağıllı rozetkalar") şəbəkədə demarkasiya nöqtələri yaratmaq və şəbəkə əlaqələrini idarə etmək, diaqnostika etmək və izləmək funksiyalarını yerinə yetirmək üçün istifadə olunan xüsusi intellektual cihazlardır (şəkil 3.20).

Ağıllı jaklar şəbəkələrin rahat və etibarlı işini təmin edən infrastrukturun mühüm elementini təmsil edirlər. Onlara adətən smart prizlər deyilir (şəkil 3.20):

- Şəbəkə interfeysi cihazları.
- Şəbəkə interfeysi blokları.
- Telefon şəbəkəsi interfeysləri.

Şəkil 3.20. Ağıllı Jaklar

Şəbəkə interfeys cihazlarının (SİC) əsas məqsədi şəbəkə interfeysi qurğuları abunəçi avadanlıqları üçün provayder şəbəkəsinə qoşulma nöqtəsi

kimi xidmət eetməkdir. SİC binanın daxili naqilləri ilə provayderdən gələn xarici rabitə əlaqəsi arasında fiziki əlaqə təmin edir. Şəbəkə interfeys cihazlarının əsas funksiyalarına aşağıdakılar daxildir:

- Xarici xətti daxili şəbəkələrdən təcrid etməklə təhlükəsizliyin təmin edilməsi.
- Şəbəkəyə qoşulmanın diaqnostikası və monitorinqi.
- Baxım üçün xəttə rahat girişin təmin edilməsi.
- Tez-tez dalğalanmadan qorunma xüsusiyyətləri daxildir.

Şəbəkə interfeysi cihazları telekommunikasiyada geniş istifadə olunur, məsələn, telefon xətlərini və ya genişzolaqlı İnterneti birləşdirmək üçün istifadə olunur.

Şəbəkə interfeysi bloklarının əsas məqsədi müxtəlif şəbəkə seqmentləri arasında körpü nöqtə rolunu oynayan, məlumat axınına nəzarət, təhlükəsizlik və monitorinq imkanı verən cihazlardır. Şəbəkə interfeysi bloklarının əsas funksiyalarına aşağıdakılar daxildir:

- Təkmil təhlükəsizlik və idarəetmə üçün şəbəkə seqmentasiyasını təmin edin.
- Ağıllı trafik təhlili üçün imkanlar.
- Uzaqdan diaqnostika və şəbəkə idarəetməsini dəstəkləyir.

Şəbəkə interfeysi blokları idarəetmə çevikliyini artırmaq üçün korporativ şəbəkələrdə, eləcə də telekommunikasiya şəbəkələrində istifadə olunur.

Telefon şəbəkəsi interfeyslərinin əsas məqsədi telefon xətlərinin binanın və ya ayrıca cihazın daxili telefon şəbəkələrinə qoşulmasını təmin edən qurğulardır. Telefon şəbəkəsi interfeyslərinin əsas funksiyalarına aşağıdakılar daxildir:

- Telefon xəttinin daxili şəbəkəyə qoşulmasının təmin edilməsi.
- Müdaxilə və həddindən artıq gərginlikdən qorunma.
- Xətt diaqnostikasının təmin edilməsi.

Telefon şəbəkəsi interfeysləri telefonları, faks maşınlarını və digər cihazları ictimai telefon şəbəkəsinə qoşmaq üçün telefon sistemlərində istifadə olunur.

YOXLAMA SUALLARI

Şəbəkə topologiyasının dizayn prosesi nələri əhatə edir?

Şəbəkə topologiyalarının əsas növləri hansılardır və onlar bir-birindən nə ilə fərqlənir?

Təşkilatınız üçün şəbəkə topologiyası seçərkən hansı amilləri nəzərə almalısınız?

Şəbəkədə fiziki bağlantılar zamanı baş verə biləcək bəzi ümumi problemlər hansılardır?

Fiziki əlaqə problemlərini müəyyən etmək və həll etmək üçün hansı alətlər və üsullardan istifadə olunur?

Şəbəkədə qısa qapanma ilə açıq dövrə arasında fərq nədir?

Qısa və açıq dövrələrin aşkarlanması və aradan qaldırılması üçün hansı üsullardan istifadə olunur?

Hansı Ethernet standartları mövcuddur və onlar bir-birindən nə ilə fərqlənir?

Məlumat ötürmə sürətləri və kabel növləri kimi Ethernet standartının əsas xüsusiyyətləri hansılardır?

Şəbəkə cihazlarını birləşdirən ənənəvi üsullarla müqayisədə WDT texnologiyasından istifadənin üstünlükləri və çatışmazlıqları hansılardır?

Ulduz, halqa, şin və qarışıq şəbəkə topologiyalarının xüsusiyyətləri hansılardır?

Hər bir şəbəkə topologiyası üçün hansı standartlar, protokollar mövcuddur?

PRAKTİKİ TAPŞIRIQ

1. Şəbəkə topologiyasının dizaynı.

Tapşırıq: Kiçik bir ofis üçün şəbəkə topologiyasının dizaynını inkişaf etdirin, təşkilatın miqyaslılıq, etibarlılıq və performans tələblərini nəzərə alın.

Məqsəd: Şəbəkəyə dair əsas prinsipləri və tələbləri nəzərə almaqla, şəbəkə infrastrukturunun layihələndirilməsi prosesini mənimsəmək.

2. Fiziki əlaqə problemlərinin müəyyən edilməsi və həlli:

Tapşırıq: Şəbəkə kabellərinin və birləşdiricilərinin tel davamlılığını yoxlamaq üçün kabel test cihazı və ya multimetrdən istifadə edin.

Məqsəd: Şəbəkə kabellərində ümumi fiziki təmas problemlərini müəyyən etmək və həll etmək üsullarını öyrənin.

3. Qısa və açıq dövrələrin aşkarlanması.

Çağırış: Şəbəkə kabellərində qısa və açıq dövrələri aşkar etmək üçün multimetrdə müqavimət testi metodundan istifadə edin.

Məqsəd: Qısa qapanma və açıq dövrə arasındakı fərqləri anlayın və onları aşkar edib aradan qaldırmağı öyrənin.

4. Ethernet standartlarına uyğun olaraq şəbəkə avadanlığının konfiqurasiyası.

Tapşırıq: Müvafiq məlumat sürətinin və kabel növünün seçilməsi kimi Ethernet tələblərinə cavab vermək üçün keçid və ya marşrutlaşdırıcınızı konfiqurasiya edin.

Məqsəd: Şəbəkə uyğunluğunu və performansını təmin etmək üçün əsas Ethernet standartlarına uyğun olaraq şəbəkə avadanlığının konfiqurasiya prosesini başa düşmək.

MODUL 4. ŞƏBƏKƏNİN İDARƏ EDİLMƏSİ

ŞƏBƏKƏNİN İDARƏ EDİLMƏSİNİN ƏSAS PRİNSİPLƏRİ
ŞƏBƏKƏNİN İDARƏ EDİLMƏSİ PARAMETRLƏRİ
MÜXTƏLİF ŞƏBƏKƏ İDARƏETMƏ ARXİTEKTURALARI
ŞƏBƏKƏ İDARƏETMƏ SİSTEMİNİN ƏSAS KOMPONENTLƏRİ
SİSTEM VƏ ŞƏBƏKƏ PROQRAMLARI
ŞƏBƏKƏ SƏNƏDLƏRİ
QoS VƏ ŞƏBƏKƏ PERFORMANSI

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

ŞƏBƏKƏNİN İDARƏ EDİLMƏSİNİN ƏSAS PRİNSİPLƏRİ

Şəbəkədə baş verənləri daim izləmək və mümkün problemləri tez bir zamanda tanımaq lazım olmasının səbəbi, şəbəkə proqramlarının müəssisələrin fəaliyyəti üçün həyati əhəmiyyətə çevrilməsidir. Şəbəkə problemlərinin işinə sərf olunan xərclər çoxlu boş iş saatları, korlanmış işgüzar münasibətlər və korlanmış ictimai imic ola bilər. Buna görə də, şəbəkə əməliyyatında və ya şəbəkə xidmətinin mövcudluğunda pozuntuları tanıya bilən alətlərə sahib olmaq lazımdır. Şəbəkə rəhbərliyi şəbəkə xidmətlərinin tələb olunan performansını və keyfiyyətini təmin etmək üçün müvafiq qiymətə şəbəkə monitorinqini, konfiqurasiyanı və təhlilini təmin etməlidir.

Şəbəkənin ümumi idarəetməsinə qoyulan tələblərə aşağıdakılar daxildir:

- Şəbəkə və xidmətlərin davamlı işləməsini təmin edin və mümkün problemləri təyini.
- Şəbəkə resurslarının icmalının və onların əlaqələrinin təyini.
- Tələb olunan texniki xidmətin icmalını təqdim edilməsi (proqram təminatı və aparat yeniləmələri).
- Şəbəkə avadanlıqlarının mərkəzləşdirilmiş konfiqurasiyasının təmin edilməsi.

Şəbəkənin idarəedilməsi funksiyaları aşağıdakı kateqoriyalara bölünür:

- Konfiqurasiyanın idarə edilməsi.
- Rəddetmələrin idarə edilməsi.
- Performansın idarə edilməsi.
- Təhlükəsizliyin idarə edilməsi.
- İstifadəçinin idarə edilməsi.
- Hesabatlılığın idarə olunması.

Rəddetmələrin idarə edilməsi (Fault Management/Breakdown Management) şəbəkədəki nasazlıqları aşkarlayan və tanıyan bir şəbəkə idarəetmə növüdür (şəkil 4.1). Müasir alətlər həmçinin nasazlığı aradan qaldırmağa və proqnozlaşdırmağa imkan verir.

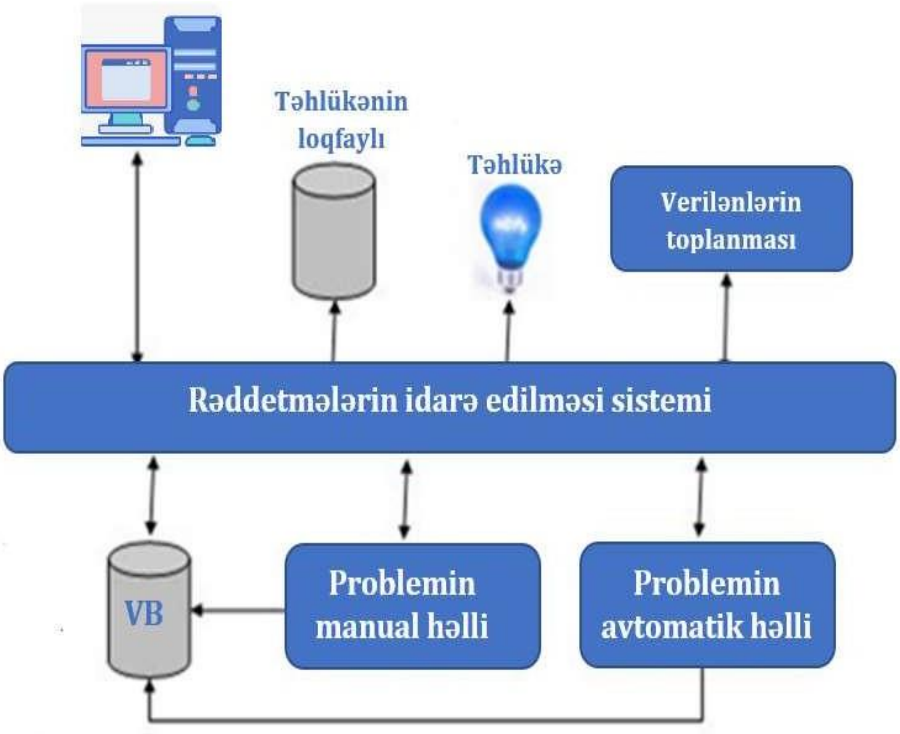
Rəddetmələrin idarə edilməsi ən azı üç mərhələdən ibarətdir:

1. Nasazlığı aşkarlamaq, onun növünü tanımaq və əhəmiyyətinə görə təsnif etmək;
2. Nasazlığın mənbəyinin təcrid edilməsi;
3. Rəddetmə mesajı göndərmək və mümkünsə, nasazlığı aradan qaldırmaq

Rəddetmələrin idarə edilməsi prosesində istifadə edilə bilən alətlərə aşağıdakılar daxildir:

1. Xəta baş verdiyi proseslər barədə administratora məlumat verən nasazlıqların aradan qaldırılması vasitələri.
2. Xətanın səbəbini göstərən təhlili vasitələri.

Cihazın proqram təminatı səviyyəsində işləyən və xəta vəziyyətlərini avtomatik həll etməyə imkan verən qabaqcıl alətlər. Məsələn, marşrutlaşdırıcının proqramı şəbəkə yolu kəsildikdə alternativ yol seçə bilir.



Şəkil 4.1. Rəddetmələrin idarə edilməsi sistemi

Eyni zamanda, bu həllər şəbəkə idarəetməsinin ümumi vasitəsi deyil, müəyyən texnologiyalara aiddir. Müasir şəbəkə idarəetmə vasitələri qrafik interfeysə və problemlərin bildirilməsi üçün müxtəlif mexanizmlərə malikdir. Problemləri effektiv şəkildə həll etmək üçün nasazlığın idarə edilməsini istifadəçi dəstəyi və problemlərin idarə edilməsi prosedurları ilə inteqrasiya etmək vacibdir.

Rəddetmələrin idarə edilməsi fəaliyyətləri konfiqurasiya idarəetmə prosesi, uzaqdan idarəetmə imkanları və müəssisə şəbəkə avadanlığı üçün konfiqurasiya parametrlərini konfiqurasiya etmək imkanı ilə dəstəklənməlidir. Bu üsulla administrator serverdə müxtəlif hadisələri və şəbəkə parametrlərini arxivləşdirə və şəbəkə avadanlıqlarına müntəzəm texniki qulluq göstərə bilər. Təhlükəsizlik baxımından hər gün parametrləri yoxlamaq və gözlədiyinizlə müqayisə etmək çox vacibdir. Bu təcrübə şəbəkə cihazlarına mümkün hücumları tez tanımağa imkan verir. Buna görə də, şəbəkə idarəetmə həlli konfiqurasiya idarəetmə alətini ehtiva etməlidir. Bu, yalnız cihazları tanıya bilən sistem qədər sadə ola bilər və ya cihaz jurnalı fayllarını yoxlaya, konfiqurasiya xətalarını aşkarlaya və cihazdan istifadə statistikasını tərtib edə bilən daha mürəkkəb sistem ola bilər.

Performansın idarə edilməsi şəbəkə qovşaqlarının və cihazlarının yükünü izləməyə və bununla da şəbəkədə tıxacları tapmağa imkan verən bir şəbəkə idarəetmə növüdür. Bu, şəbəkə cihazlarının, onların istifadəsinin və şəbəkə infrastrukturunun tələblərə cavab verib-vermədiyini yoxlamaq yolu ilə həyata keçirilir. O, həmçinin şəbəkə avadanlığından səmərəli istifadə üçün siyasətlərin müəyyən edilməsi üçün lazımi məlumatları təqdim etməklə performansın planlaşdırılması prosesinə töhfə verir. Performansın idarəetməsi aşağıdakıları əhatə edir:

- Cihazdan istifadə statistikasının toplanması.
- Bildiriş həddinin müəyyən edilməsi.
- Hər növ sınaq və simulyasiya prosedurları.
- Hesabatlılıq.

Performansın idarəetməsini tətbiq etmək üçün aşağıdakı parametləri qiymətləndirmək lazımdır:

- Zaman vahidinə və cəminə ötürülən məlumatların həcmi
- Sorğu, emal və cavab vaxtlarının əlavə edilməsi ilə hesablanan pik saatlarda cihazların və xidmətlərin cavab müddəti.
- Həddindən artıq yükləmə səbəbindən rədd edilən sorğuların faizi
- İki xəta arasındakı orta vaxt kimi ölçülən mövcudluq
- Baxım üçün qeyri-pik vaxtları müəyyənləşdirilməsi.

Təhlükəsizliyin idarə edilməsi mümkün hücumları və digər təhlükəsizlik təhdidlərini müəyyən etmək, qarşısını almaq və onlara qarşı çıxmaq üçün müxtəlif şəbəkə idarəetmə alətləri və sistemlərindən istifadə edir. Şəbəkə təhlükəsizliyinin təmin edilməsi infrastruktur üçün vacib olan və ya işçilərin şəxsi məlumatlarının məxfiliyinə aid olan məlumatların müəyyən edilməsi ilə

başlayır. Sonra bütün giriş kanallarını, məsələn, terminal xidmətləri, FTP, HTTP serverləri, şəbəkənin ayrılması və onlara girişin təmin edilməsi ilə bağlı hər bir prosesi, o cümlədən DNS kimi infrastruktur xidmətlərini müəyyən etmək lazımdır. Məlumat təhlükəsizliyinin təmin edilməsi müxtəlif səviyyələrdə həyata keçirilə bilər:

- Məlumat bağlantısı səviyyəsində kriptoqrafiyadan istifadə edərək mühafizə;
- Şəbəkə səviyyəsində, yalnız seçilmiş trafikə icazə verir, bunun üçün paketləri süzür;
- Tətbiq səviyyəsində, təhlükəsiz və SƏRT autentifikasiya proseduru vasitəsilə mühafizə.

Eyni zamanda, şəbəkə administratoru heç bir prosesin lazımi xidmətlərin işləməsinə və mövcudluğuna mane olmamasını təmin etməlidir, yəni. xidmətləri inkar etməyə yönəlmiş hücumları tanıyır. Təhlükəsizliyin idarə olunması mümkün hücumların, məlumatların oğurlanması və ya dəyişdirilməsi cəhdlərinin qarşısını almalıdır və ya xidmətləri bloklamalıdır. Buna nail olmaq üçün təhlükəsizlik idarəetmə sistemi məlumatların istifadəsini tez və effektiv şəkildə nümayiş etdirmək üçün nəzarət və izləmə sistemləri ilə təchiz olunmalıdır.

Nəzarət sistemləri cəhdləri və ya hücumları izləməklə və bu barədə administratora məlumat verməklə icazəsiz girişin qarşısını alır. İzləmə mexanizminin növündən asılı olaraq mühafizə vasitələri aktiv və passiv bölünə bilər. Passiv alətlər müəyyən vaxt intervallarında şəbəkənin cari vəziyyətini izləməyə imkan verir. Proaktiv alətlər davamlı olaraq xidmət və cihazların istifadəsini real vaxtda ölçə və şübhəli fəaliyyətə xəbərdarlıqlar və ya konfiqurasiya dəyişiklikləri ilə cavab verə bilər.

Ayrı-ayrı istifadəçilər tərəfindən şəbəkə resurslarının istifadəsinə də nəzarət etmək lazımdır. Bu məlumatlara əsaslanaraq, siz şəbəkədə istifadəçi yükünü müəyyən edə və lazım olduqda şəbəkə tıxanmasının qarşısını almaq üçün şəbəkə trafikinə cavab verə və prioritetləşdirə bilərsiniz. Məsələn, siz VoIP trafikinə üstünlük verməli və fayl endirmələri ilə əlaqəli trafiki məhdudlaşdırmalısınız. Şəbəkə idarəetmə trafikinin hərəkət etdiyi şəbəkə mühitinin növündən asılı olaraq, şəbəkə idarəetmə sistemləri xüsusi şəbəkə infrastrukturuna malik avtonom (oflayn) və idarəetmə trafikinin eyni mühitdən keçdiyi daxili (daxili) bölünə bilər. şəbəkənin qalan hissəsi kimi. Məsələn, şəbəkə trafikinin parametrlərini ölçmək üçün ölçülən eyni şəbəkəni idarə etmək üçün istifadə etmək məntiqlidir.

ŞƏBƏKƏNİN İDARƏ EDİLMƏSİ PARAMETRLƏRİ

Şəbəkə texnologiyaları müasir informasiya infrastrukturunda əsas rol oynayır, qurğular, istifadəçilər və xidmətlər arasında əlaqə yaradır. Şəbəkə idarəçiliyinə inzibatçıya şəbəkə resurslarının dayanıqlığını, təhlükəsizliyini və səmərəliliyini qorumağa imkan verən bir sıra prosedurlar, alətlər və parametrlər daxildir. Şəbəkənin effektiv idarə edilməsi təkcə biznesin davamlığını təmin etmir, həm də infrastrukturu dəyişən tələblərə uyğunlaşdırmağa, mümkün insidentlərin qarşısını almağa və xidmət keyfiyyətinin yüksək səviyyəsini təmin etməyə imkan verir.

Şəbəkə idarəetmə parametrləri administratorlara şəbəkə avadanlığının və şəbəkə xidmətlərinin performansını idarə etməyə, izləməyə və optimallaşdırmağa imkan verən parametrlər və konfiqurasiyalar toplusudur. Bu parametrlər şəbəkə arxitekturasının müxtəlif aspektlərini əhatə edir, məsələn, marşrutlaşdırma, IP ünvanlama, təhlükəsizlik, girişə nəzarət, xidmətin idarə edilməsinin keyfiyyəti və s. Bu parametrlərin düzgün konfiqurasiyası yüksək yük şəraitində səmərəli fəaliyyət göstərə bilən və resurslara təhlükəsiz çıxışı təmin edən çevik və möhkəm şəbəkə yaratmağa imkan verir.

- Şəbəkə idarəetmə parametrləri aşağıdakılar üçün tələb olunur.
- Şəbəkənin etibarlılığını və davamlılığını təmin edilməsi.
- Şəbəkənin təhlükəsiz saxlanması.
- Resursdan istifadənin optimallaşdırılması.
- İdarəetməni sadələşdirinlməsi.
- Çeviklik və miqyaslılığın təmin edilməsi.

Şəbəkə avadanlığının və xidmətlərinin düzgün işləməsinin təmin edilməsi dayanma vaxtı və məlumat itkisi risklərini minimuma endirir. Firewall, VPN-lər və trafik filtrasiyası kimi təhlükəsizlik parametrləri şəbəkənizi xarici təhlükələrdən və icazəsiz girişdən qoruyur. Trafikin idarə edilməsi, yük balansı və QoS şəbəkə resurslarını səmərəli şəkildə bölüşdürməyə imkan verir, ümumi şəbəkə performansını yaxşılaşdırır. Avtomatlaşdırma və mərkəzləşdirilmiş şəbəkə idarəetməsi quraşdırma, monitorinq və problemlərin aradan qaldırılması prosesini xeyli asanlaşdıra bilər. Düzgün konfiqurasiya edilmiş şəbəkə istifadəçilərin sayının artması, topologiyanın dəyişməsi və ya yeni xidmətlərin tətbiqi kimi yeni tələblərə asanlıqla uyğunlaşa bilər.

Şəbəkə idarəetmə parametrlərinə şəbəkə avadanlığının və ümumilikdə şəbəkələrin işini idarə etməyə və optimallaşdırmağa imkan verən müxtəlif parametrlər və konfiqurasiyalar daxildir:

1. IP ünvanlama və alt şəbəkə maskaları.
2. Marşrutlaşdırma.
3. DNS (Domen Adı Sistemi).
4. DHCP (Dinamik Host Konfiqurasiya Protokolu).
5. NAT (Şəbəkə Ünvanının Tərcüməsi).
6. VLAN (Virtual Lokal Şəbəkə).
7.QoS (Xidmət keyfiyyəti).
8. Firewall və giriş qaydaları.
9. SNMP (Simple Network Management Protocol).
10. VPN (Virtual Şəxsi Şəbəkə).
11. SSID və simsiz şəbəkənin idarə edilməsi.
12. Şəbəkə trafikinin monitorinqi və təhlili.

IP ünvanlama və alt şəbəkə maskaları cihazların şəbəkə identifikasiyası və onların qarşılıqlı əlaqəsi üçün əsasdır. IP ünvanlarının və alt şəbəkə maskalarının düzgün konfiqurasiyası sizə şəbəkənizi alt qruplara bölməyə imkan verir, trafikin idarə edilməsini və təhlükəsizliyi təkmilləşdirir. Bu, həmçinin ünvan münaqişələrinin qarşısını almağa kömək edir və şəbəkədəki cihazların düzgün əlaqə saxlamasını təmin edir.

Şəbəkələr arasında məlumatların ötürülməsində marşrutlaşdırma əsas rol oynayır. Paketləri mənbədən təyinat yerinə ötürmək üçün optimal yolu seçmək üçün məsuliyyət daşıyır. Marşrutlaşdırma parametrləri şəbəkəni dəyişən şərtlərə uyğunlaşdırmağa və məlumatların ötürülməsində gecikmələri minimuma endirməyə imkan verən statik və ya dinamik marşrutların istifadəsini əhatə edir.

DNS (Domain Name System) domen adlarını IP ünvanlarına həll edir, rəqəmsal ünvanlar deyil, adlar vasitəsilə resurslara asan giriş imkanı verir. DNS serverlərinin konfiqurasiyası sürətli və etibarlı ad həllini təmin edir ki, bu da şəbəkənin sabit işləməsi və resurslara qoşulma zamanı gecikmələrin minimuma endirilməsi üçün vacibdir.

DHCP (Dynamic Host Configuration Protocol) şəbəkədəki cihazlara IP ünvanlarının və digər şəbəkə parametrlərinin təyin edilməsini avtomatlaşdırır. Bu, hər bir qovşağın əl ilə konfiqurasiyasının son dərəcə əlverişsiz olacağı geniş miqyasda şəbəkə idarəetməsini asanlaşdırır. DHCP serverləri müvəqqəti olaraq ünvanlar təyin edir və məhdud IP resurslarından səmərəli istifadə etməyə imkan verir.

NAT (Şəbəkə Ünvanının Tərcüməsi) sizə daxili şəbəkə infrastrukturunuzu bir və ya bir neçə ictimai IP ünvanının arxasında gizlətməyə imkan verir. Xarici qurğular daxili ünvanlara birbaşa daxil ola bilmədiyi üçün bu, təhlükəsizliyi yaxşılaşdırır və həmçinin bir neçə cihaz üçün bir ünvandan istifadə etməklə IP ünvanlarını saxlamağa kömək edir.

VLAN (Virtual Lokal Şəbəkə) fiziki şəbəkəni çoxsaylı məntiqi şəbəkələrə bölməyə imkan verir. Bu, müxtəlif trafik növlərini ayırmağa və fiziki əlaqələrdən daha çox məntiqi qruplar əsasında şəbəkələr arasında girişi idarə etməyə imkan verməklə trafikin idarə edilməsini asanlaşdırır, təhlükəsizliyi artırır və performansını artırır.

QoS (Xidmətin Keyfiyyəti) şəbəkədəki trafikin prioritetlərini idarə edərək, səsli və ya video zənglər kimi kritik əhəmiyyət kəsb edən tətbiqlərə daha az vacib məlumatlar üzərində üstünlük verilməsini təmin edir. Bu, gecikməni minimuma endirmək və zəng keyfiyyətini yaxşılaşdırmaq üçün məhdud bant genişliyi mühitlərində xüsusilə vacibdir.

Firewall və giriş qaydaları bir sıra qaydalar əsasında daxil olan və gedən trafikə nəzarəti təmin edir. O, IP ünvanı, port və protokol növü kimi müxtəlif parametrlər əsasında trafiki süzərək şəbəkənizi icazəsiz giriş və təhdidlərdən qorumağa kömək edir.

SNMP (Sadə Şəbəkə İdarəetmə Protokolu) şəbəkə administratorlarına şəbəkə avadanlıqlarını izləmək və idarə etmək imkanı verir. SNMP-dən istifadə edərək, siz cihazın sağlamlıq məlumatlarını toplaya və şəbəkə sabitliyini və təhlükəsizliyini qorumağa kömək edən nasazlıqlar və ya anomaliyalar barədə avtomatik məlumat verə bilərsiniz.

VPN (virtual özəl şəbəkə) ötürülən məlumatların məxfiliyini və bütövlüyünü təmin edərək, ictimai şəbəkələr üzərində təhlükəsiz bağlantılar yaradır. VPN şifrələməni və dünyanın istənilən yerindən resurslara təhlükəsiz girişi təmin edərək korporativ şəbəkələrə uzaqdan bağlantıları təmin etmək üçün istifadə olunur.

SSID və simsiz şəbəkənin idarə edilməsinə simsiz şəbəkə identifikatorlarının (SSID) qurulması və Wi-Fi təhlükəsizliyi və girişinin idarə edilməsi daxildir. Simsiz parametrlərə istifadəçi identifikasiyası, məlumat şifrələməsi və MAC ünvanına əsaslanan giriş nəzarəti daxil ola bilər.

Şəbəkə təhlükəsizliyini və performansını təmin etmək üçün şəbəkə trafikinin monitorinqi və təhlili vacibdir. Monitorinqdən istifadə edərək, siz real vaxt rejimində fəaliyyəti izləyə, anomaliyaları və darboğazları müəyyən edə,

sonrakı təhlil və şəbəkə performansının optimallaşdırılması üçün statistika toplaya bilərsiniz.

Bu parametrlər şəbəkə administratoruna şəbəkə infrastrukturunun dayanıqlığını, təhlükəsizliyini və səmərəliliyini izləməyə və saxlamağa imkan verir.

MÜXTƏLİF ŞƏBƏKƏ İDARƏETMƏ ARXİTEKTURALARI

İnformasiya texnologiyalarının inkişafı və şəbəkə infrastrukturlarının mürəkkəbliyi ilə yeni yanaşmalar və şəbəkə idarəetmə arxitekturaları yaranır. Bu arxitekturalar komponentlərin təşkili və qarşılıqlı əlaqəsi ilə fərqlənir ki, bu da onlara miqyaslılıq, təhlükəsizlik, idarəetmənin asanlığı və uyğunlaşmanın çevikliyi kimi xüsusi problemləri həll etməyə imkan verir. Müxtəlif şəbəkə idarəetmə arxitekturalarını başa düşmək müxtəlif əməliyyat mühitlərində etibarlı və təhlükəsiz kommunikasiyaları təmin edən müasir şəbəkələrin effektiv layihələndirilməsi və istismarı üçün vacibdir.

Şəbəkə idarəetmə arxitekturaları şəbəkə komponentlərinin necə təşkil olunduğunu və qarşılıqlı əlaqəsini müəyyən edən konseptual modellər və diaqramlardır. Əsas memarlıqlara aşağıdakılar daxildir:

- Mərkəzləşdirilmiş arxitektura.
- Mərkəzləşdirilməmiş (paylanmış) arxitektura.
- İyerarxik arxitektura.
- Proqram təminatı ilə müəyyən edilmiş şəbəkələrə (SDN) əsaslanan idarəetmə arxitekturası.

Mərkəzləşdirilmiş arxitektura şəbəkə vahid mərkəzdən idarə olunur, burada bütün idarəetmə qərarları və əməliyyatlar bir yerdə cəmlənir. Mərkəzləşdirilmiş nəzarətçilər şəbəkə cihazlarını və protokollarını idarə edir, vahid nəzarət və monitorinqi təmin edir.

Mərkəzləşdirilməmiş bir arxitekturada idarəetmə funksiyaları bir neçə şəbəkə qovşağı arasında paylanır. Hər bir cihaz və ya qurğular qrupu öz idarəetmə funksiyalarını yerinə yetirə bilər ki, bu da bir uğursuzluq nöqtəsindən asılılığı azaldır və sistemin dayanıqlığını artırır.

İyerarxik arxitektura həm mərkəzləşdirilmiş, həm də qeyri-mərkəzləşdirilmiş idarəetmə elementlərini birləşdirir, onları təbəqələrə təşkil edir. Üst təbəqə şəbəkənin daha qlobal aspektlərinə nəzarət edir, aşağı təbəqələr isə daha çox yerli məsələlərlə məşğul olur.

Proqram təminatı ilə müəyyən edilmiş şəbəkələrə (SDN) əsaslanan idarəetmə arxitekturası proqram təminatından istifadə edərək şəbəkənin mərkəzləşdirilmiş şəkildə idarə olunmasına imkan verən idarəetmə funksiyalarını (idarəetmə təbəqəsi) verilənlər səviyyəsindən (keçid qatı) ayırır. Bu, real vaxt rejimində şəbəkənin idarə edilməsində və konfiqurasiyasında çeviklik təmin edir.

Şəbəkə idarəetmə arxitekturaları sistemə aşağıdakı üstünlükləri qazandırır:

1. Şəbəkənin idarə edilməsini və əməliyyatını optimallaşdırılması – düzgün arxitekturanın seçilməsi şəbəkə idarəetmə prosesini sadələşdirməyə kömək edir, onu cari tapşırıqlara və iş yükünə daha səmərəli və uyğunlaşdırmağa imkan verir.
2. Davamlılığın artırılması – mərkəzləşdirilməmiş və iyerarxik arxitekturalar mərkəzi qovşaqların nasazlığı ilə bağlı riskləri azaldır, hətta uğursuzluq şəraitində belə şəbəkənin davamlılığını təmin edir.
3. Çeviklik və miqyaslılığı təmin edilməsi – SDN və iyerarxik modellər şəbəkəni dəyişən biznes tələblərinə uyğunlaşdırmağı və əhəmiyyətli xərclər və idarəetmə mürəkkəbliyi olmadan genişləndirməyi asanlaşdırır.
4. Təhlükəsizliyin təkmilləşdirilməsi – nəzarət arxitekturaları şifrələmə, girişə nəzarət və anomaliyaların monitorinqi kimi təhlükəsizlik nəzarətlərini mərkəzləşdirilmiş şəkildə həyata keçirməyə və izləməyə kömək edir.
5. Əməliyyat xərclərini azaldılması – müvafiq arxitektura ilə şəbəkə idarəetmə proseslərinin optimallaşdırılması şəbəkə infrastrukturunun istismarı, idarə edilməsi və saxlanması xərclərini azaldır.

ŞƏBƏKƏ İDARƏETMƏ SİSTEMİNİN ƏSAS KOMPONENTLƏRİ

Ümumiyyətlə, şəbəkə idarəetmə sistemi aşağıdakı komponentlərdən ibarətdir:

1. Şəbəkə idarəetmə konsolu;
2. Agentlərlə idarə olunan cihazlar;
3. Şəbəkə idarəetmə protokolu.

Şəbəkə idarəetmə konsolu şəbəkə administratorları üçün şəbəkənin bütün aspektlərini izləmək və idarə etmək üçün əsas interfeys nöqtəsidir. O, şəbəkə performansına nəzarət etmək, parametrləri konfiqurasiya etmək, problemləri həll etmək və təhlükəsizlik siyasətlərini idarə etmək imkanı verir.

Agentləri olan idarə olunan cihazlar daxili agentlər vasitəsilə idarəetməni dəstəkləyən şəbəkə cihazlarıdır (məsələn, marşrutlaşdırıcılar, açarlar, serverlər). Agentlər cihaz vəziyyəti məlumatlarının toplanmasına və idarəetmə konsolundan göndərilən əmrlərin yerinə yetirilməsinə cavabdehdirlər.

Şəbəkə idarəetmə protokolu idarəetmə konsolu ilə idarə olunan cihazlar arasında məlumatların necə ötürüləcəyini müəyyən edən qaydalar və standartlar toplusudur. Belə protokollara misal olaraq SNMP (Simple Network Management Protocol), NetFlow və başqalarını göstərmək olar. Protokollar şəbəkə idarəetmə sisteminin bütün elementləri arasında qarşılıqlı əlaqəni təmin edərək, administratora şəbəkəni effektiv idarə etməyə və nəzarət etməyə imkan verir.

İdarə olunan qurğular dəstinə iş stansiyaları, serverlər, splitterlər, açarlar, şlüzlər və marşrutlaşdırıcılar kimi bütün aktiv şəbəkə qurğuları daxildir. Bu cihazlarda performans və əməliyyat məlumatlarını toplayan xüsusi proqram modulu və ya agent var. Agentlər bu məlumatı İMB (İdarəetmə Məlumatı Bazasında) saxlayırlar. Agentlər, İMB-lər və konsol şəbəkə idarəetmə sistemlərini təşkil edir. İMB agentlərdən alınan məlumatların toplandığı xüsusi verilənlər bazasıdır.

İMB və şəbəkə idarəetmə sistemi arasında məlumat mübadiləsi SNMP (Simple Network Management Protocol) kimi şəbəkə idarəetmə protokolundan istifadə etməklə həyata keçirilir. Agent, cihazda problemi tanıyan kimi dərhal idarəetmə blokuna həyəcan siqnalı göndərir, bu da bir və ya bir neçə hərəkəti yerinə yetirir, məsələn, operatora mesaj göndərir, hadisə məlumatlarını saxlayır, sistemi bağlayır və avtomatik olaraq xətanın səbəbini müəyyən etməyə çalışır. İdarəetmə bloku həmçinin avtomatik və ya operator vasitəsilə əlavə məlumat toplaya bilər.

Şəbəkə idarəetmə sisteminin arxitekturası paylanmış və ya mərkəzləşdirilmiş ola bilər. Mərkəzləşdirilmiş şəbəkə idarəetmə sistemi ilə bütün idarəetmə sistemi şəbəkənin bir sahəsində cəmləşmişdir ki, bu da çox vaxt müəssisənin idarəetmə mərkəzidir. Agentlər şəbəkə daxilində paylanır və pinglər və SNMP sorğularına cavablar kimi məlumatları mərkəzi idarəetmə blokuna göndərirlər. Məlumat ötürülməsi ya xüsusi şəbəkə, ya da işləyən şəbəkə üzərindən baş verə bilər.

Paylanmış şəbəkə idarəetmə sistemi o deməkdir ki, şəbəkə idarəetmə xidmətləri və agentləri bütün şəbəkədə paylanır. Bu halda iyerarxik idarəetmədən istifadə oluna bilər, bu halda iyerarxiyada daha aşağı olan şəbəkə idarəetmə sistemləri məlumatları mərkəzi idarəetmə sisteminə göndərirlər.

Bu, məlumatların mərkəzi idarəetmə sisteminə göndərilməzdən əvvəl aşağı səviyyələrdə süzülməsinə imkan verir və bununla da artıq nəzarət trafikini məhdudlaşdırır. Paylanmış sistemin digər üstünlüyü ondan ibarətdir ki, sistemin hissələri uğursuz olsa belə, məlumatların toplanması davam edir. Paylanmış şəbəkə idarəetmə sisteminin dezavantajı arxitektura və idarəetmənin mürəkkəbliyidir.

SNMP - SADƏ ŞƏBƏKƏ İDARƏETMƏ PROTOKOLU

Şəbəkə trafikinin təhlili[29] kompüter şəbəkələrinin təhlükəsizliyinin və səmərəliliyinin təmin edilməsində əsas rol oynayır. Şəbəkə trafikinə nəzarət etməklə siz anomaliyaları, şübhəli fəaliyyətləri və məlumat sızmalarını müəyyən edə bilərsiniz. Bu proses şəbəkə üzərindən ötürülən məlumatların toplanması, təhlili və şərh edilməsini əhatə edir. Şəbəkə trafikini təhlil etməklə hücumları, virusları, DDoS hücumlarını və digər təhlükəsizlik təhdidlərini aşkar etmək və qarşısını almaq olar. Avadanlıqların nasazlıqları müəyyən edildikdən sonra, şəbəkənin işində fasilələri və fasilələri minimuma endirmək üçün onlar aradan qaldırılır. İnfrastrukturun sabit və təhlükəsiz işini təmin etmək üçün şəbəkə trafikinin müntəzəm auditinin aparılması vacibdir. Bu yanaşma potensial təhlükələrin və uğursuzluqların qarşısını almağa kömək edir, şəbəkənin düzgün işləməsini təmin edir.

SNMP (Sadə Şəbəkə İdarəetmə Protokolu) və SYSLOG hadisələrin qeydiyyatı sistemi kompüter şəbəkələrinin və cihazlarının monitorinqi və idarə edilməsi üçün iki mühüm vasitədir. SNMP marşrutlaşdırıcılar, açarlar, serverlər və digər şəbəkə cihazları kimi şəbəkə cihazlarını uzaqdan izləmək və idarə etmək üçün istifadə olunur. SNMP-dən istifadə edərək, administratorlar cihazın

[29] https://moodle.kstu.ru/mod/page/view.php?id=9364
https://www.coursera.org/courses?query=information%20security
https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords
https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
https://blog.kaspersky.com/10-worst-password-ideas-as-seen-in-the-adobe-hack/3198/
http://lifehacker.com/5937303/your-clever-password-tricks-arent-protecting-you-from-todays-hackers
https://www.random.org/passwords/
http://world.std.com/~reinhold/diceware.html
https://www.safetydetectives.com/password-meter/
http://www.pcworld.com/article/2858642/you-can-encrypt-your-hard-drive-but-the-protection-may-not-be-worth-the-hassle.html

statusu haqqında məlumat əldə edə və uzaqdan konfiqurasiya və idarəetməni həyata keçirə bilərlər. SYSLOG, digər tərəfdən, müxtəlif cihaz və sistemlərdən hadisə qeydlərini toplamaq, saxlamaq və təhlil etmək üçün istifadə olunan standart bir hadisə qeydi protokoludur. Bu, idarəçilərə şəbəkə fəaliyyətlərinə və hadisələrə, o cümlədən xətalar, xəbərdarlıqlar, uğurlu və uğursuz giriş cəhdləri və digər mühüm hadisələrə nəzarət etməyə imkan verir. SNMP və SYSLOG birlikdə etibarlı və təhlükəsiz şəbəkəni təmin etmək üçün problemləri aşkarlamağa, izləməyə və onlara tez cavab verməyə kömək edən hərtərəfli şəbəkə monitorinqi və idarəetmə mexanizmini təmin edir.

SNMP (Sadə Şəbəkə İdarəetmə Protokolu) administratora şəbəkə cihazlarının parametrlərini dəyişməyə və ya idarə etməyə imkan verən əməliyyatlar dəstindən ibarət şəbəkə idarəetmə protokoludur. Məsələn, SNMP-dən istifadə edərək, idarəçi marşrutlaşdırıcının şəbəkə interfeysini söndürə və ya onun sürətini təyin edə bilər. SNMP-nin sələfi marşrutlaşdırıcıları idarə etmək üçün nəzərdə tutulmuş SGMP (Simple Gateway Management Protocol) idi. SGMP-nin baza kimi istifadə edilməsinin səbəbləri aşağıdakılardır:

Agent əməliyyatının mürəkkəbliyini azaldın ki, bu da öz növbəsində proqram təminatının hazırlanması xərclərini azaldacaq, eyni texnologiyanın müxtəlif qurğular üçün istifadəsinə imkan verəcək və agentlərin özlərini birbaşa dəyişdirmədən agentlərin funksional imkanlarını genişləndirmək imkanı verəcək.

- Məlumat ölçülərini asanlıqla əlavə etmək imkanı.
- Xüsusi şəbəkə arxitekturasından müstəqillik.
- Sürətli məlumat ötürülməsi üçün müstəqil şəbəkə protokollarını dəstəkləyir.
- Digər şəbəkə xidmətlərindən müstəqillik.

İdarə olunan obyektlər ağac iyerarxiyasında təşkil edilir. SNMP adlandırma sxemi bu struktura əsaslanır. Hər bir obyektin idarə olunan obyektin adını unikal şəkildə müəyyən edən öz OID-i var. Adlar iki formada təqdim olunur: ədədi və insan tərəfindən oxuna bilən format. Hər halda, SNMP proqramlarını hazırlayarkən adlar uzun və əlverişsiz olur, istifadəçini ad sahəsində rahat naviqasiya ilə necə təmin edəcəyinizi düşünməlisiniz. Obyekt identifikatoru ağacın budaqlanmasına uyğun olaraq tam ədədlərin nöqtəli ardıcıllığından ibarətdir. İnsan tərəfindən oxuna bilən formatda obyekt identifikatoru nöqtələrlə ayrılmış seriya adlarından ibarətdir.

SNMP versiyaları. SNMP (Sadə Şəbəkə İdarəetmə Protokolu) hər biri əvvəlki versiyalarla müqayisədə funksionallıq, təhlükəsizlik və performansda

təkmilləşdirmələr təklif edən bir neçə versiyada gəlir. SNMP-nin əsas versiyalarına baxaq:

1. SNMPv1 – 1988-ci ildə təqdim edilən SNMP protokolunun ilk versiyasıdır. O, marşrutlaşdırıcılar, açarlar və serverlər kimi şəbəkə cihazları üçün əsas monitorinq və idarəetmə funksiyalarını təmin edir. Bununla belə, SNMPv1 məhdud təhlükəsizlik imkanlarına malikdir, çünki o, aydın mətnlə göndərilən "icma sətri"nə əsaslanan sadə autentifikasiya mexanizmindən istifadə edir. Bu, SNMPv1-ni məlumatların tutulmasına və icazəsiz girişə qarşı həssas edir.

2. SNMPv2c – Protokolun ikinci versiyası 1993-cü ildə təqdim edilib və təkmilləşdirilmiş performans xüsusiyyətlərini ehtiva edir və böyük həcmli məlumatların səmərəli şəkildə əldə edilməsinə imkan verən GetBulk kimi yeni əməliyyat növləri əlavə edir. Bununla belə, SNMPv1 kimi, SNMPv2c versiyası da eyni icma simli əsaslı təhlükəsizlik modelindən istifadə edir ki, bu da onu hücumlara qarşı həssas edir.

3. SNMPv3 – 1998-ci ildə buraxılmış bu versiya əhəmiyyətli təhlükəsizlik təkmilləşdirmələri təklif edir. SNMPv3 autentifikasiya, şifrələmə və girişə nəzarət kimi anlayışları təqdim edərək onu müasir şəbəkələrdə istifadə üçün daha təhlükəsiz edir. Bu versiyada məlumatlar şifrələnmiş şəkildə ötürülür və autentifikasiya parol əsaslı metodlardan istifadə etməklə həyata keçirilir. SNMPv3 həmçinin şəbəkə cihazlarına girişi çevik şəkildə konfiqurasiya etməyə imkan verən istifadəçi və rolun idarə edilməsini dəstəkləyir.

Versiyalar arasındakı əsas fərqlər aşağıdakı kimidir: SNMPv1–

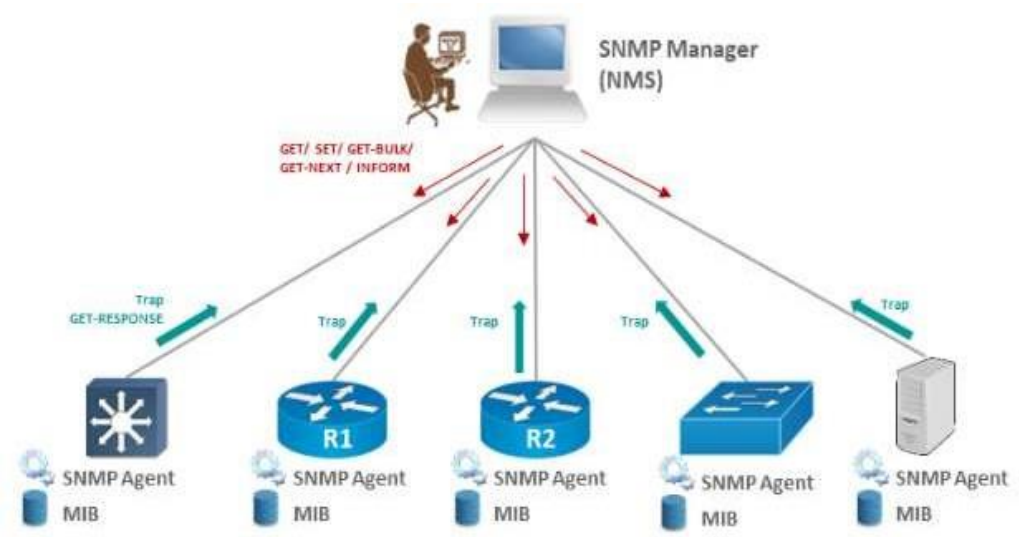
Əsas funksionallıq, minimal təhlükəsizlik (açıq mətn).

SNMPv2c – Təkmilləşdirilmiş performans, lakin SNMPv1 ilə eyni təhlükəsizlik modeli.

SNMPv3 – Doğrulama, şifrələmə və giriş nəzarəti ilə təkmilləşdirilmiş təhlükəsizlik.

SNMPv3 təkmilləşdirilmiş təhlükəsizlik xüsusiyyətlərinə görə əksər müasir şəbəkələr üçün üstünlük verilən versiyadır. SNMP-nin əsas bölmələri menecerlər və agentlərdir. Menecer, şəbəkə idarəetmə tapşırıqlarını yerinə yetirməyə qadir olan müəyyən bir proqram növü ilə işləyən bir serverdir. Menecerlər çox vaxt şəbəkə idarəetmə stansiyaları adlanır (NMS – Network Management Station). NMS agentlərə məlumat (Sorğu) göndərir və onlardan fasilələr (Trap) alır. Şəbəkə terminologiyasında Sorğu sözü agentə məlumat sorğusu göndərmək deməkdir. Toplanmış məlumat şəbəkə problemlərini həll etmək üçün istifadə edilə bilər.

Trap, agentin problemli vəziyyət barədə meneceri xəbərdar etməsi üsuludur. Agentlər Tələləri menecer sorğusuna cavab olaraq deyil, asinxron şəkildə göndərirlər. Menecer alınan məlumatla sonra nə edəcəyinə qərar verir. Məsələn, İnternet bağlantısı kəsilirsə, agent menecerə Trap mesajı göndərir və menecer öz administratoru ilə birlikdə yata bilər (SMS, e-poçt və s. vasitəsilə). Agent idarə olunan şəbəkə cihazında işləyən kompüter proqramıdır. Agent ya ayrıca proqram ola bilər, ya da əməliyyat sisteminə inteqrasiya oluna bilər (məsələn, marşrutlaşdırıcının və ya UPS-in proqram təminatına). Sorğu və Trap eyni vaxtda yaradıla bilər (şəkil 4.2).



Şəkil 4.2. SNMP strukturu

SNMP xidmətləri. SNMP-də (Sadə Şəbəkə İdarəetmə Protokolu) hər bir əməliyyat idarə olunan cihazlar və idarəetmə stansiyaları arasında həyata keçirilən müxtəlif növ əməliyyatları təsvir edən standart PDU (Protokol Məlumat Vahidi) formatına malikdir.

- Get.
- GetNext.
- GetBulk (SNMPv2 və ya SNMPv3).
- Set.
- GetResponse.
- Trap.

- Notification (SNMPv2 və ya SNMPv3).
- Inform (SNMPv2 və ya SNMPv3).
- Report (SNMPv2 və ya SNMPv3).

Get cihazın İMB-dən (İdarəetmə Məlumatı Bazasından) dəyərləri əldə etmək üçün istifadə edilən əsas əmrdir. Bu əməliyyat OID (Obyekt İdentifikatoru) tərəfindən müəyyən edilmiş xüsusi bir obyekti sorğulayır və onun cari dəyərini qaytarır, idarəçilərə cihaz statusu haqqında məlumat əldə etməyə imkan verir.

GetNext, İMB iyerarxiyasında növbəti obyektin dəyərini əldə etməyə imkan verən Get əmrinin genişləndirilməsidir. Bu əməliyyat MIB ağacını keçmək lazım olduqda faydalıdır, çünki o, əvvəlcədən obyektlərin dəqiq OID-lərini bilmədən məlumatları ardıcıllıqla əldə etməyə imkan verir.

GetBulk (SNMPv2-də təqdim olunur və SNMPv3-də dəstəklənir) - böyük həcmli məlumatların daha səmərəli şəkildə əldə edilməsi üçün nəzərdə tutulmuşdur. Bu əmr bir əməliyyatda çoxlu obyektləri sorğulayır ki, bu da tələb olunan sorğuların sayını azaldır və böyük həcmli məlumatlarla işləyərkən performansı yaxşılaşdırır.

Set idarə olunan cihazın İMB-dəki obyektlərin dəyərlərini dəyişdirmək üçün istifadə edilən bir əmrdir. Onun köməyi ilə administrator uzaqdan avadanlıq parametrlərini konfiqurasiya edə bilər ki, bu da administratorlara şəbəkə cihazlarını idarə etməyə imkan verir.

GetResponse idarə olunan cihazdan Get, GetNext, GetBulk və Set əmrlərinə cavab mesajıdır. O, tələb olunan məlumatları və ya əmrin müvəffəqiyyətlə tamamlanmasının təsdiqini, habelə varsa, səhvlər haqqında məlumatları ehtiva edir.

Trap aparat xətaları və ya cihaz vəziyyətindəki dəyişikliklər kimi əhəmiyyətli hadisələr və ya problemlər barədə bildiriş vermək üçün idarə olunan cihaz tərəfindən idarəetmə stansiyasına göndərilən asinxron mesajdır. Digər əmrlərdən fərqli olaraq, Trap idarəetmə stansiyasından sorğu tələb etmir.

Bildiriş (SNMPv2-də əlavə edilib və SNMPv3-də dəstəklənir) hadisə bildirişləri də göndərən, lakin genişləndirilmiş imkanlara malik olan Trap-ın analoqudur. Bildiriş əlavə parametrləri və daha çevik strukturu ehtiva edir ki, bu da bildirişlərin göndərilməsini və hadisələrin idarə edilməsini tənzimləməyə imkan verir.

Inform (SNMPv2-də təqdim olunur və SNMPv3-də dəstəklənir) Trap-in təkmilləşdirilmiş versiyasıdır və o, təkcə hadisə bildirişi göndərmir, həm də idarəetmə stansiyasından təsdiq gözləyir. Bu, nəzarət sisteminin etibarlılığını artıraraq bildirişin qəbul edilməsini və işlənməsini təmin edir.

Hesabat (SNMPv3-də əlavə edilmişdir) - agentlər və idarəetmə stansiyaları arasında SNMP mesajlarının emalı ilə bağlı problemlər haqqında məlumat mübadiləsi üçün istifadə olunur. Bu əmr agentlərə xətalar və ya protokol uyğunsuzluqları baş verdikdə idarəetmə stansiyalarını xəbərdar etməyə imkan verir ki, bu da problemlərin aradan qaldırılmasına və şəbəkə sabitliyini qorumağa kömək edir.

Bu PDU standartları şəbəkə qurğularının səmərəli idarə edilməsinə və monitorinqinə imkan verir, inzibatçıları şəbəkə infrastrukturu ilə qarşılıqlı əlaqədə olmaq və optimallaşdırmaq üçün geniş alətlərlə təmin edir.

SNMP sorğuları. SNMP sorğuları şəbəkədə idarəetmə stansiyaları (menecerlər) və idarə olunan qurğular (agentlər) arasında əlaqə yaratmaq üçün istifadə edilən əmrlərdir. Onlar administratorlara şəbəkə statusu haqqında məlumat əldə etməyə, aparat parametrlərini dəyişməyə və hadisələrə nəzarət etməyə imkan verir. Get sorğusu idarə olunan cihazın İMB-dən (İdarəetmə Məlumatı Bazasından) məlumat almaq üçün istifadə olunur. Bu, idarəetmə stansiyasının prosessor yükü, yaddaş istifadəsi və ya interfeys statusu kimi cihaz parametrlərinin cari vəziyyəti haqqında məlumat əldə etdiyi əsas sorğudur. GetNext sorğusu obyekt iyerarxiyasında növbəti girişi tələb etməklə ardıcıl olaraq İMB-dən məlumatları əldə etməyə imkan verir. Bu sorğu İMB cədvəlində çoxlu əlaqəli obyektləri keçmək lazım olduqda, məsələn, cihazdakı bütün interfeyslər haqqında məlumat toplamaq üçün faydalıdır. Set sorğusu idarə olunan cihazın parametrlərini dəyişdirmək üçün nəzərdə tutulub. Onun köməyi ilə siz şəbəkə avadanlıqlarını uzaqdan konfiqurasiya edə bilərsiniz, məsələn, IP ünvanını dəyişdirə, marşrutu konfiqurasiya edə və ya müəyyən funksiyaları aktivləşdirə bilərsiniz. Bu, avadanlıqlara fiziki giriş olmadan dəyişikliklər etməyə imkan verən güclü şəbəkə idarəetmə vasitəsidir. GetResponse sorğusu idarə olunan cihazdan Get, GetNext və ya Set əmrlərinə cavab mesajıdır. Bu cavabda idarəetmə stansiyası tərəfindən tələb olunan məlumatlar və ya mümkün səhvlər də daxil olmaqla yerinə yetirilən əmrin nəticəsi haqqında məlumat var. Tələ sorğusu idarə olunan cihazın özü tərəfindən başlanır və mühüm hadisələr və ya problemlər barədə bildiriş vermək üçün idarəetmə stansiyasına göndərilir. Bu asinxron mesaj hardware

nasazlıqları, həddindən artıq yüklənmələr və ya administratorun diqqətini tələb edən digər anomaliyalar barədə xəbərdarlıq etmək üçün istifadə olunur.

Məlumat sorğusu Trap sorğusunun təkmilləşdirilmiş versiyasıdır və hadisələr haqqında onların alınmasının təsdiqi ilə bildirişlər göndərmək üçün istifadə olunur. Bu, nəzarət stansiyasının bildiriş aldığını və müvafiq tədbirlər görə biləcəyini təmin edir. Məlumat sorğuları şəbəkə monitorinqi və idarəetmə sisteminin etibarlılığını artırır. Hesabat sorğusu SNMP sorğularının emalı ilə bağlı səhvlər və ya digər problemlər haqqında mesajlar göndərmək üçün istifadə olunur. O, agentlər və idarəetmə stansiyaları arasında diaqnostik məlumat mübadiləsi üçün istifadə olunur, şəbəkənin sabitliyini və düzgün işləməsini qorumağa kömək edir. Bu sorğular şəbəkə infrastrukturunun tam idarə edilməsini və monitorinqini təmin edərək, administratorlara məlumatları tez əldə etməyə, avadanlıqları konfiqurasiya etməyə və insidentlərə cavab verməyə imkan verir.

SİSTEM VƏ ŞƏBƏKƏ PROQRAMLARI

Müasir kompüter sistemləri və şəbəkələrinin fəaliyyətində sistem və şəbəkə proqram təminatı əsas rol oynayır. Bu sahəyə giriş sizə aparat resurslarını idarə edən və cihazlar arasında əlaqə saxlayan proqram komponentlərinin əsas anlayışlarını və iş prinsiplərini başa düşməyə kömək edir. Sistem proqram təminatına əməliyyat sistemləri, qurğu drayverləri və kompüterin əsas funksiyalarını idarə edən utilitlər daxildir. Əməliyyat sistemləri istifadəçi və aparat arasında qarşılıqlı əlaqəni təmin edir, prosesləri, yaddaş və fayl sistemlərini idarə edir və tətbiqi proqramların işləməsi üçün platforma təmin edir. Cihaz drayverləri printerlər, video kartlar və sərt disklər kimi müxtəlif periferik cihazların düzgün işləməsinə, onların əməliyyat sistemi ilə uyğunluğunun təmin edilməsinə cavabdehdir. Şəbəkə proqramı kompüterlər və şəbəkədəki digər qurğular arasında əlaqə yaratmaq üçün nəzərdə tutulmuşdur. Buraya şəbəkə əməliyyat sistemləri, rabitə protokolları və şəbəkə utilitləri daxildir. Windows Server və Linux kimi şəbəkə əməliyyat sistemləri fayllar, printerlər və verilənlər bazası kimi şəbəkə resurslarının idarə edilməsi üçün platforma təmin edir və bu resurslara girişin təhlükəsizliyini və nəzarətini təmin edir. TCP/IP kimi rabitə protokolları məlumatların şəbəkə

üzərindən ötürülməsi qaydalarını müəyyən edir, məlumatın etibarlılığını və bütövlüyünü təmin edir.

Sistem və şəbəkə proqram təminatından istifadənin məqsədi kompüter sistemlərinin və şəbəkələrinin işini optimallaşdırmaqdır. Sistem proqram təminatı kompüterinizin resurslarını idarə edir, proqramların səmərəli icrasını təmin edir və məlumatların mühafizəsini təmin edir. Şəbəkə proqramı, öz növbəsində, məlumatların ötürülməsini və resurslara çıxışı dəstəkləyən şəbəkədəki cihazların rəvan qarşılıqlı əlaqəsini təmin edir. Bunun sayəsində şirkətlər və istifadəçilər məlumatların işlənməsi, məlumatların saxlanması və əməkdaşlıq kimi müxtəlif vəzifələri həll etmək üçün kompüter sistemlərindən səmərəli istifadə edə bilərlər.

Ümumiyyətlə, sistem və şəbəkə proqram təminatı istənilən kompüter sistemlərinin və şəbəkələrinin fəaliyyətinin əsasını təşkil edir, idarəetmə, rabitə və təhlükəsizlik üçün lazımi alətləri təmin edir.

Sistem və şəbəkə proqram təminatı bir neçə növə bölünə bilər ki, onların hər biri kompüter sistemlərinin və şəbəkələrinin işini təmin etmək üçün xüsusi funksiyaları yerinə yetirir. Sistem proqram təminatına kompüterin işləməsi üçün əsas olan əməliyyat sistemləri daxildir. Əməliyyat sistemləri kompüterin bütün resurslarını, o cümlədən prosessorları, yaddaşı, disk sürücülərini və periferiya qurğularını idarə edir. Onlar həmçinin aparat və tətbiq proqramları arasında qarşılıqlı əlaqəni təmin edərək proqramların işləməsi üçün mühit yaradırlar. Windows, macOS və Linux kimi əməliyyat sistemləri bu tip proqram təminatına misaldır. Sistem proqram təminatının başqa bir növü faylların idarə edilməsi, təhlükəsizlik və sistemin optimallaşdırılması kimi kommunal tapşırıqları yerinə yetirən kommunal proqramlardır. Utilitlər kompüterinizin işləməsini təmin etmək üçün antivirus proqramlarını, məlumatların ehtiyat nüsxəsini çıxaran proqramları, disk defraqmentatorlarını və digər alətləri əhatə edə bilər.

Şəbəkə proqram təminatı, öz növbəsində, şəbəkə əməliyyat sistemlərinə, şəbəkə protokollarına və şəbəkə utilitlərinə bölünür. Windows Server və Linux kimi şəbəkə əməliyyat sistemləri şəbəkə resurslarını idarə edir və cihazlar arasında əlaqəni təmin edir. Onlar faylları, printerləri və digər resursları paylaşmaq, həmçinin istifadəçiləri və şəbəkə təhlükəsizliyini idarə etmək üçün funksiyalar təmin edir. TCP/IP kimi şəbəkə protokolları məlumatların şəbəkə üzərindən ötürülməsi qaydalarını və prosedurlarını müəyyən edir. Bu protokollar internetin və lokal şəbəkələrin fəaliyyəti üçün əsas olan

məlumatların etibarlı çatdırılmasını və şəbəkə əlaqələrinin idarə edilməsini təmin edir.

Şəbəkə yardım proqramlarına şəbəkənin monitorinqi və idarə edilməsi üçün proqramlar daxildir. Bu cür kommunal proqramlara misal olaraq şəbəkə trafikinin monitorinqi, şəbəkə problemlərinin diaqnostikası və girişin idarə edilməsi üçün proqramlar daxildir. Bu yardım proqramları idarəçilərə şəbəkələri idarə etməyə kömək edir, onların sabitliyini və təhlükəsizliyini təmin edir. Beləliklə, sistem və şəbəkə proqram təminatının növləri həm fərdi kompüterlərin, həm də bütün şəbəkələrin işini idarə etmək və optimallaşdırmaq üçün lazım olan geniş funksiyaları əhatə edir.

Ümumi şəbəkə idarəetmə proqramları. Ümumi şəbəkə idarəetmə proqramı şəbəkə resurslarını izləmək, idarə etmək və optimallaşdırmaq üçün nəzərdə tutulmuş alətlər və proqramlardır. Bu proqramlar administratorlara şəbəkə performansını izləmək, problemləri həll etmək, girişi idarə etmək və təhlükəsizliyi təmin etmək imkanı verir. Şəbəkə monitorinq proqramı marşrutlaşdırıcılar, açarlar və serverlər daxil olmaqla şəbəkədəki bütün cihazların işinə nəzarət edir. O, trafik, gecikmə və resurs istifadəsi kimi şəbəkə performansı məlumatlarını toplayır, idarəçilərə problemləri müəyyən etməyə və kəsilmələrə səbəb olmamışdan əvvəl onları həll etməyə imkan verir. Belə proqram təminatına misal olaraq Nagios, SolarWinds və PRTG Network Monitor daxildir. Şəbəkə konfiqurasiyasının idarə edilməsi proqramları şəbəkə cihazı parametrlərinin mərkəzləşdirilmiş idarə edilməsini təmin edir. Bu alətlər administratorlara marşrutlaşdırıcılarda, açarlarda və digər cihazlarda konfiqurasiya dəyişiklikləri etməyə və onların statusuna nəzarət etməyə imkan verir. Cisco Network Assistant və Ansible kimi proqram təminatı idarəetmə proseslərini avtomatlaşdırmağa və xəta riskini minimuma endirməyə kömək edir.

Şəbəkə təhlükəsizliyini təmin etmək üçün resurslara girişi idarə edən, təhdidlərdən qoruyan və təhlükəsizlik siyasətlərini idarə edən proqramlardan istifadə olunur. Bu cür proqramlara müdaxiləyə qarşı alətlər, müdaxilənin aşkarlanması və qarşısının alınması sistemləri (IDS/IPS) və firewall idarəetmə proqramı daxildir. Nümunələrə Palo Alto Networks, Fortinet və Cisco Secure daxildir. VMware NSX və Microsoft Azure Network Watcher kimi virtual şəbəkə idarəetmə proqramı administratorlara virtual marşrutlaşdırıcılar və açarlar kimi virtuallaşdırılmış şəbəkə resurslarını idarə etməyə və izləməyə imkan verir. Bu alətlər mürəkkəb şəbəkələrin idarə edilməsini sadələşdirir və miqyasda çeviklik təmin edir.

Bundan əlavə, simsiz şəbəkələrinizə mərkəzləşdirilmiş nəzarəti təmin edən Cisco Meraki və Ubiquiti UniFi kimi Wi-Fi şəbəkə idarəetmə proqramları mövcuddur. Bu həllər Wi-Fi performansını optimallaşdırmağa, giriş nöqtələrini idarə etməyə və simsiz bağlantıları qorumağa kömək edir.

Beləliklə, ümumi şəbəkə idarəetmə proqramı geniş spektrli vəzifələri əhatə edir - monitorinq və konfiqurasiya idarəetməsindən təhlükəsizlik və şəbəkə optimallaşdırılmasına qədər. Bu alətlər sabit, təhlükəsiz və səmərəli şəbəkə infrastrukturunu saxlamaq üçün vacibdir. Müxtəlif şəbəkə idarəetmə proqramlarına nümunələr:

Spiceworks: http://www.spiceworks.com/

OpenNMS: http://www.opennms.org/

Nagios: http://www.nagios.org

Zabbix:: http://www.zabbix.com/

Şəbəkə idarəetmə proqramlarını işə salmaq üçün infrastruktur tələbləri. Böyük bir şəbəkəni idarə etmək üçün NMS sistemi kifayət qədər güclü olmalıdır. Şəbəkə ölçüsü bir neçə cihazdan bir neçə min cihaza qədər dəyişə bilər. Mesaj mübadiləsi və emalı güclü avadanlıq tələb edir. Əvvəlcə şəbəkə idarəetmə sistemi istehsalçısından server konfiqurasiyası tövsiyəsi almalısınız. Əksər istehsalçılarda tələb olunan aparat konfiqurasiyasının hesablandığı xüsusi düsturlar var. Düsturlar idarə olunan cihazların sayını, toplamaq istədiyim məlumatların miqdarını və məlumat sorğularının tezliyini nəzərə alır. Tutaq ki, məsələn, 1000 cihazımız var və biz onlardan hər dəqiqə məlumat toplamaq istəyirik və hər cihaz üçün məlumat həcmi 1 kB-dir. Bu, dəqiqədə 1 MB, gündə 1,4 GB və ayda 40 GB-a bərabərdir. Bu məlumatların həcmi məlumatların toplanması intervalını azaltmaqla, monitorinq üçün yalnız kritik cihazları (serverlər, açarlar, marşrutlaşdırıcılar və s.) və yalnız ən vacib məlumatları seçməklə azaldıla bilər.

ŞƏBƏKƏ SƏNƏDLƏRİ

Şəbəkə sənədləri kompüter şəbəkələrinin planlaşdırılması, idarə edilməsi və saxlanması üçün mühüm vasitədir. Bunlara şəbəkə diaqramları, cihazın texniki xüsusiyyətləri, təhlükəsizlik siyasətləri, şəbəkə diaqramları və konfiqurasiya sənədləri kimi müxtəlif sənədlər daxildir. Bu sənədlər administratorlara şəbəkə strukturunu başa düşməyə, aparat və proqram

təminatı tələblərini müəyyən etməyə, təhlükəsizlik və məlumatların ehtiyat nüsxəsini çıxarmaq strategiyalarını inkişaf etdirməyə kömək edir. Şəbəkə sənədləri həmçinin işçilərin təlimi və üçüncü tərəflərə məlumat verilməsi üçün əsas rolunu oynayır. Müvafiq sənədlər olmadan şəbəkənin idarə edilməsi və saxlanması çətin ola bilər, ona görə də aktual və ətraflı sənədlərin saxlanılması peşəkar şəbəkə idarəçiliyinin əsas aspektidir. Şəbəkə sənədləri aşağıdakıları əhatə edir:

- Kabel diaqramları.
- Şəbəkə kartları.
- Kabel idarəetmə.
- Aktivlərin idarə olunması.
- Baza xətləri.
- Dəyişik idarəetmə.

Şəbəkə sənədlərinə kompüter şəbəkələrinin planlaşdırılması, idarə edilməsi və saxlanması üçün zəruri olan müxtəlif növ sənədlər daxildir. Sənədləşdirmənin əsas elementlərindən biri kabel diaqramlarıdır. Bu diaqramlar şəbəkənin fiziki topologiyasını göstərir, cihazların kabellər vasitəsilə bir-birinə necə qoşulduğunu göstərir. Bu, idarəçilərə bütün şəbəkə elementlərinin necə bağlandığını dəqiq anlamağa kömək edir, problemlərin diaqnostikasını və yeni əlaqələri planlaşdırmağı asanlaşdırır.

Şəbəkə kartları da şəbəkənin idarə olunmasında mühüm rol oynayır. Onlar marşrutlaşdırıcılar, açarlar və serverlər kimi şəbəkə cihazları arasındakı yeri və əlaqələri göstərən şəbəkənin məntiqi strukturunu vizuallaşdırırlar. Bu xəritələr administratorlara məlumatların şəbəkə üzrə necə axdığını anlamağa kömək edir və marşrutları optimallaşdırmaq və performansı yaxşılaşdırmaq üçün əsas yaradır.

Kabel idarəetməsi sənədlərin başqa bir vacib aspektidir. Buraya əlaqələri müəyyən etmək və saxlamağı asanlaşdırmaq üçün kabellərin təşkili və etiketlənməsi daxildir. Kabelin düzgün idarə edilməsi şəbəkə xətaları ehtimalını azaldır və sizə lazım olan bağlantılara daxil olmağı asanlaşdırır.

Aktivlərin idarə edilməsi bütün şəbəkə cihazlarını və avadanlıqlarını izləmək və sənədləşdirməkdən ibarətdir. Bu, idarəçilərə şəbəkədə hansı cihazların olduğunu, harada yerləşdiyini və hansı vəziyyətdə olduqlarını tam şəkildə görməyə imkan verir. Bu sənədlər resursların effektiv idarə edilməsi və təkmilləşdirmənin planlaşdırılması üçün vacibdir.

Əsas göstəricilərə ötürmə qabiliyyəti, gecikmə və resurs istifadəsi kimi şəbəkə performansı məlumatları daxildir. Bu ölçülər şəbəkə performansını

təhlil etmək və izləmək üçün sənədləşdirilmişdir. Bu göstəriciləri müntəzəm olaraq yeniləmək və izləmək sizə potensial problemləri müəyyən etməyə və onları həll etmək üçün tədbirlər görməyə kömək edir.

Dəyişikliklərin idarə edilməsi şəbəkə sənədlərinin vacib hissəsidir. O, avadanlıq təkmilləşdirmələri, konfiqurasiya dəyişiklikləri və ya yeni təhlükəsizlik siyasətlərinin həyata keçirilməsi kimi şəbəkəyə edilən bütün dəyişiklikləri qeyd etməyi əhatə edir. Bu, dəyişikliklərin tarixini izləməyə kömək edir və onların şəbəkəyə necə təsir göstərməsinə nəzarət edir.

Bu sənədlər birlikdə şəbəkə infrastrukturu üzərində tam nəzarəti təmin edir, onu optimal vəziyyətdə saxlamağa imkan verir və şəbəkənin təhlükəsizliyinə və sabitliyinə zəmanət verir.

QoS VƏ ŞƏBƏKƏ PERFORMANSI

Xidmətin keyfiyyəti (QoS) və şəbəkə performansı, xüsusən də trafik artdıqca və şəbəkə proqramları daha müxtəlifləşdikcə, şəbəkə idarəçiliyinin vacib aspektləridir. QoS kritik tətbiqlərin etibarlı işləməsinin təmin edilməsində və şəbəkə performansının yüksək standartlarının saxlanmasında əsas rol oynayır.

QoS şəbəkədə trafikə üstünlük verməyə imkan verən, müəyyən növ məlumatlara zəmanətli xidmət keyfiyyətini təmin edən texnologiyalar və mexanizmlər toplusudur. Məsələn, korporativ şəbəkələrdə video konfrans, səsli zənglər və digər real vaxt proqramları müntəzəm məlumat ötürülməsi və ya fayl endirilməsi ilə müqayisədə daha yüksək prioritetlər tələb edə bilər. QoS, ən kritik tətbiqlər üçün gecikmələri və paket itkisini minimuma endirəcək şəkildə bant genişliyini paylayaraq, trafikin prioritetləşdirilməsi siyasətini qurmağa imkan verir.

Şəbəkənin performansı QoS ilə sıx bağlıdır, çünki şəbəkənin keyfiyyəti onun resurslarının effektiv idarə olunmasından asılıdır. Şəbəkə performansı ötürmə qabiliyyəti, gecikmə, cavab müddəti və paket itkisi kimi parametrlərlə ölçülür. Bu parametrlər şəbəkə sıxlığının səviyyəsindən və onun arxitekturasından asılı olaraq əhəmiyyətli dərəcədə dəyişə bilər. Məsələn, böyük həcmdə məlumat ötürmək üçün yüksək ötürmə qabiliyyəti tələb olunur, aşağı gecikmə isə sürətli cavab müddəti tələb edən proqramlar üçün vacibdir.

QoS sıxlığın təsirini minimuma endirməklə və əsas tətbiqlər üçün resurslara prioritet girişi təmin etməklə şəbəkə performansını yaxşılaşdırır.

Məsələn, QoS olmadan, video və səsli zəngləri eyni vaxtda yayımlayan bir çox cihazın olduğu şəbəkədə gecikmələr və keyfiyyətin pisləşməsi baş verə bilər. QoS növbənin idarə edilməsi və bant genişliyi bölgüsü mexanizmlərini tətbiq etməklə, kritik tətbiqlərin rəvan işləməsini təmin edərək, bu problemlərin qarşısını alır.

QoS-in mühüm hissəsi trafikin monitorinqi və nəzarətidir. Buraya müxtəlif trafik növləri üçün bant genişliyi məhdudiyyətlərinin təyin edilməsi, tıxacların idarə edilməsi və resursların bərabər paylanmasının təmin edilməsi daxildir. Optimal şəbəkə performansına nail olmaq üçün idarəçilərə şəbəkənin sağlamlığına nəzarət etməyə və QoS parametrlərini operativ şəkildə tənzimləməyə imkan verən monitorinq və təhlil alətləri tələb olunur.

Beləliklə, QoS və şəbəkə performansı şəbəkə infrastrukturunun səmərəliliyini müəyyən edən bir-biri ilə əlaqəli elementlərdir. QoS tənzimləməsi və performansa daimi diqqət sabit şəbəkəni saxlamağa kömək edir və bütün istifadəçilər və proqramlar üçün yüksək keyfiyyətli təcrübə təmin edir.

YOXLAMA SUALLARI

1. Müasir şəbəkələrdə hansı növ şəbəkə avadanlıqlarından istifadə olunur?
2. Kommutatorlar, marşrutlaşdırıcılar və təhlükəsizlik divarları kimi şəbəkə avadanlıqlarının əsas funksiyaları hansılardır?
3. Hansı səbəblər şəbəkə avadanlığının nasazlığına səbəb ola bilər?
4. Şəbəkə avadanlıqlarının diaqnostikası və nasazlıqlarının aradan qaldırılması üçün hansı üsullardan istifadə olunur?
5. Şəbəkə aparat proqram təminatı ilə baş verə biləcək tipik problemlər hansılardır?
6. Proqram təminatı problemlərini müəyyən etmək və həll etmək üçün hansı alət və üsullardan istifadə olunur?
7. SNMP nədir və bu protokol şəbəkənin idarə edilməsi üçün hansı xüsusiyyətləri təmin edir?
8. Şəbəkə problemlərini aşkar etmək və həll etmək üçün Syslog və şəbəkə trafikinin təhlilindən nə istifadə olunur?

9. Şəbəkə infrastrukturunu sənədləşdirmək üçün hansı növ sənədlərdən istifadə olunur?

10. Şəbəkə sənədlərinə hansı məlumatlar, məsələn, şəbəkə diaqramları, konfiqurasiya təlimatları və s. daxil edilməlidir?

11. QoS (Xidmətin Keyfiyyəti) nədir və o, şəbəkə performansına necə təsir edir?

12. Yüksək QoS səviyyəsini təmin etmək və şəbəkə performansını optimallaşdırmaq üçün hansı üsul və texnologiyalardan istifadə olunur?

PRAKTİKİ TAPŞIRIQ

1. Şəbəkə avadanlıqlarının identifikasiyası və təsnifatı.

Məqsəd: Şəbəkə avadanlığının müxtəlif növlərini, məsələn, açarlar, marşrutlaşdırıcılar, firewalllar və VPN marşrutlaşdırıcıları öyrənin və onların əsas xüsusiyyətlərini və funksiyalarını müəyyənləşdirin.

Məqsəd: Şəbəkə avadanlıqlarının növləri arasındakı fərqləri və onların müasir şəbəkələrdə necə istifadə edildiyini başa düşmək.

2. Şəbəkə avadanlıqlarının diaqnostikası və nasazlıqların aradan qaldırılması.

Tapşırıq: Ping, traceroute və SNMP kimi alətlərdən istifadə edərək şəbəkə avadanlığının diaqnostikasını aparın.

Məqsəd: Şəbəkə avadanlıqlarının diaqnostikası üsullarını mənimsəmək və ümumi problemlərin aradan qaldırılması yollarını öyrənmək.

3. Sistem jurnalı ilə işləmək və şəbəkə trafikini təhlil etmək.

Tapşırıq: şəbəkə problemlərini izləmək və təhlil etmək üçün Wireshark kimi syslog və şəbəkə trafikinin təhlili alətlərini konfiqurasiya edin.

Məqsəd: Şəbəkə problemlərini aşkar etmək və həll etmək üçün monitorinq və təhlil alətlərindən istifadə prosesini öyrənin.

4. Şəbəkə sənədlərinin yaradılması.

Tapşırıq: Şəbəkə diaqramlarını, konfiqurasiya təlimatlarını, avadanlıq siyahılarını və satıcı ilə əlaqə məlumatlarını ehtiva edən şəbəkə sənədlərini hazırlayın.

Məqsəd: Şəbəkə infrastrukturunun sənədləşdirilməsinin vacibliyini anlayın və şəbəkəyə texniki xidmət üçün faydalı sənədlərin necə yaradılacağını öyrənin.

MODUL 5. ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNƏ GİRİŞ

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN ƏSAS MƏQSƏDİ, PREDMETİ VƏ VƏZİFƏLƏRİ
ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN NÖVLƏRİ
ŞƏBƏKƏ TƏHLÜKƏSIZLİYİ ÜÇÜN ALƏTLƏR
ƏN YAXŞI ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ SERTİFİKATLARI
İT İNFRASTRUKTURUNUN YARADILMASI PRİNSİPLƏRİ
ŞƏBƏKƏ PERİMETRİNİN TƏHLÜKƏSİZLİYİNİN QURULMASI METODOLOGİYASI

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN ƏSAS MƏQSƏDİ, PREDMETİ VƏ VƏZİFƏLƏRİ

Şəbəkə təhlükəsizliyi nədir?

Şəbəkə təhlükəsizliyi[30] şəbəkə resurslarının və məlumatlarının bütövlüyünü, məxfiliyini və əl çatanlığını qorumağa yönəlmiş informasiya təhlükəsizliyi sahəsidir. Başqa sözlə desək, Əksər ekspertlər şəbəkə təhlükəsizliyini şəbəkə infrastrukturunu müdaxilədən, qeyri-qanuni girişdən, modifikasiyadan, sui-istifadədən, dəyişdirmədən, məhv etməkdən və ya icazəsiz məlumatların toplanması və yayılmasından qorumaq üçün qoruyucu tədbirlərin görülməsi siyasəti və təcrübələri kimi müəyyən edirlər. Tam proses hardware cihazlarının, təhlükəsizlik proqram təminatının və istifadəçinin təhlükəsizlik prosedurları və texnikaları haqqında məlumatlılığının birləşməsini tələb edir. Sonuncu element müvafiq təhlükəsizlik təcrübələri haqqında məlumatlandırılan işçilərdən tutmuş şəbəkə təhlükəsizliyi üzrə təlim keçmiş mütəxəssislərə qədər dəyişə bilər. Onda qarşıya belə bir sual çıxır:

Şəbəkə təhlükəsizliyi nə üçün lazımdır?

Həyatımızın bir çox aspektləri rəqəmsal dünyaya inteqrasiya edib. Biz internetdən maliyyə əməliyyatları aparmaq, ailə və həmkarlarımızla ünsiyyət qurmaq, alış-veriş etmək, əyləncə axtarmaq və araşdırma aparmaq üçün istifadə edirik. Şəxsi məlumatlarımızın çoxu onlayndır, doğum tarixlərindən, Sosial Müdafiədən (və ya digər identifikasiya nömrələrindən), sağlamlıq tarixçəsindən, kredit tarixçəsindən, bank hesablarından, kommunal ödənişlərdən və s. Bütün bu məlumatlar və əməliyyatlar hakerlər və kibercinayətkarlar qarşısında həssasdır. Ömrümüzü nə qədər çox internetə həsr etsək, güzəşt riski bir o qədər yüksək olar. Üstəlik, Əşyaların İnternetinin (IoT) davamlı tətbiqi simsiz şəbəkələrə daha çox etibar etmək deməkdir ki, bu da yalnız təhlükə mənzərəsini artırır, cinayətkarlara fırıldaqçılıq etmək üçün daha çox yol və imkanlar verir. Şəbəkə təhlükəsizliyini pozulması şəxsi və biznes həyatımızın sıradan çıxamasına dəlalət edir.

---

[30] Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.

Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. М.: Форум, Инфра-М, 2017. 416 с.

Mark Ciampa. CompTIA® Security+ Guide to Network Security Fundamentals, Seventh EditionCengage Learning, Inc. 2022, WCN: 02-300

Şəbəkə təhlükəsizliyinin əsas məqsədi. Şəbəkə təhlükəsizliyinin əsas məqsədi verilənlərə və resurslara icazəsiz girişin qarşısını almaq və məlumatların şəbəkələr arasında təhlükəsiz ötürülməsini təmin etməkdir. Şəbəkə təhlükəsizliyi həmçinin zərərli proqramların və hücumların təsirinin qarşısının alınmasına, normativ tələblərə əməl olunmasına və informasiya təhlükəsizliyi risklərinin idarə olunmasına diqqət yetirir.

Şəbəkə təhlükəsizliyinin predmeti. Şəbəkə təhlükəsizliyinin predmeti təhlükəsizlik təhdidlərinə həssas ola bilən şəbəkə sistemləri və komponentləridir. Buraya daxildir:

- Şəbəkə cihazları və avadanlıqları – şəbəkə infrastrukturunun mühüm komponentidir və şəbəkələrin əlaqə və funksionallığının təmin edilməsində əsas rol oynayır. Bu texniki vasutələrə router, kommutator, firewall, Hub, switch və s.

- Proqram təminatı sistemi – əməliyyat sistemləri, server proqram təminatı, tətbiq proqramları, verilənlər bazası və şəbəkə mühitində işləyən digər proqramları əhatə edir.

- Şəbəkə protokolları və kommunikasiyalar – TCP/IP, HTTP, FTP, SMTP və şəbəkə üzərindən məlumat ötürmək üçün istifadə olunan digər protokollar aiddir.

- Şəbəkə infrastrukturu – Şəbəkənin fiziki və məntiqi strukturu, o cümlədən kabellər, açarlar, marşrutlaşdırıcılar, serverlər, yaddaş və digər şəbəkə resursları.

- Siyasətlər və prosedurlar – Giriş qaydalarını, zəifliyin idarə edilməsini, insidentlərə reaksiyanı və şəbəkə təhlükəsizliyinin idarə edilməsinin digər aspektlərini müəyyən edən qaydalar, siyasətlər, standartlar və prosedurlar.

Beləliklə, şəbəkə təhlükəsizliyi predmeti şəbəkə resurslarının və məlumatların təhdid və hücumlardan qorunması, həmçinin şəbəkə infrastrukturunun təhlükəsiz və etibarlı fəaliyyətinin təmin edilməsi ilə bağlı bütün aspektləri əhatə edir.

Şəbəkə təhlükəsizliyinin əsas vəzifələri – qarşıya qoyulan məqsədə çatmaq üçün şəbəkə təhlükəsizliyi xidmətinin üzərinə şəbəkə infrastrukturunun təhlükəsizliyinin təmin edilməsinə, məlumatların təhdid və hücumlardan qorunmasına yönəlmiş bir sıra vəzifələri əhatə edir. Bu vəzifələr aşağıdakılardır:

- Təhlükəsizlik siyasətlərinin inkişafı.
- Şəbəkə təhlükəsizliyi monitorinqi.
- Təhlükəsizlik insidentinə cavab.

- Zəifliyin idarə edilməsi.
- Uyğunluğun təmin edilməsi.
- Təlim və maarifləndirmə.

Şəbəkə təhlükəsizliyi şəbəkə və məlumatların təhlükəsizliyini təmin etmək üçün zəruri olan qaydaları, siyasətləri və prosedurları müəyyən edir. Buraya təhlükəsizlik standartlarının təyin edilməsi, giriş qaydalarının yaradılması və məxfilik siyasətlərinin idarə edilməsi daxildir. Şəbəkə təhlükəsizliyi monitorinqi şəbəkənin xidmət fəaliyyətinə nəzarət edir və onu anomaliyalar və potensial təhlükələr üçün təhlil edir. Bura qeyri-adi trafik nümunələrinin axtarışı, müdaxilənin aşkarlanması və hadisə qeydlərinin təhlili daxildir.

Təhlükəsizlik insidentinə cavab hücum və ya məlumat sızması kimi bir təhlükəsizlik hadisəsi aşkar edildikdə, şəbəkə təhlükəsizlik komandası hücumu dayandırmaq, pozulmuş təhlükəsizliyi bərpa etmək və hadisənin nəticələrini yumşaltmaq üçün dərhal cavab verir.

Zəifliyin idarə edilməsi xidmət şəbəkə infrastrukturunda zəiflikləri təhlil edir və onları aradan qaldırmaq və ya azaltmaq üçün strategiyalar hazırlayır. Buraya proqram təminatının yamaqlanması, cihaz konfiqurasiyalarının yenilənməsi və risklərin idarə edilməsi tədbirlərinin həyata keçirilməsi daxil ola bilər.

Uyğunluğun təmin edilməsi şəbəkə təhlükəsizliyi informasiya təhlükəsizliyi qaydalarına və standartlarına uyğunluğu təmin edir. Təlim və Maarifləndirməyə təlimlərin keçirilməsi və şəbəkə resursları ilə işləyərkən təhlükəsiz təcrübələrdən istifadə etmək üçün işçi heyətinin hazırlanması daxildir. Bu və digər şəbəkə təhlükəsizliyi öhdəlikləri təşkilatın şəbəkə infrastrukturu və məlumatlarının etibarlılığını, bütövlüyünü və məxfiliyini təmin etməyə kömək edir.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN NÖVLƏRİ

Şəbəkə təhlükəsizliyi adətən fiziki, texniki və inzibati tədbirlər də daxil olmaqla müxtəlif üsul və texnologiyaların kombinasiyası vasitəsilə həyata keçirilir.

Fiziki Təhlükəsizlik - informasiya sisteminin fiziki resurslarının, məsələn, server otaqlarının, kompüterlərin, şəbəkə avadanlıqlarının və s. mühafizəsi ilə

bağlıdır. Fiziki təhlükəsizlik tədbirlərinə icazəsiz girişin qarşısını almaq üçün binalara nəzarət edilən giriş, kilidlərdən istifadə, videomüşahidə, biometrik sistemlər və digər fiziki maneələr daxildir. Fiziki təhlükəsizliyin əsas elementləri aşağıdakılardır:

- Girişə nəzarət.
- Video müşahidə.
- Təhlükəsizlik siqnalları.
- Fiziki maneələr.
- İşıqlandırma.
- İşçilərin maarifləndirilməsi.
- Fiziki avadanlıq dəstəyi.

Server otaqları, məlumat mərkəzləri və s. kimi fiziki yerlərə girişi idarə edin və məhdudlaşdırır. Bura açarların, elektron giriş kartlarının, biometrik sistemlərin (barmaq izləri, sifətin tanınması və s.) və giriş sistemlərinin istifadəsi daxil ola bilər. Binalara nəzarət etmək və insanların hərəkətinə nəzarət etmək üçün CCTV kameralarının quraşdırılması, Video qeydlər təhlükəsizlik insidentlərini araşdırmaq və sübut təqdim etmək üçün istifadə edilə bilər. İcazəsiz giriş və ya müdaxilə cəhdi zamanı avtomatik işə salına bilən təhlükəsizlik siqnalizasiya sistemlərinin quraşdırılması daxildir. Bu sistemlərə hərəkət sensorları, qapı və pəncərələrdə kontakt sensorları, tüstü aşkarlama sistemləri və s. daxil ola bilər. Binalara və avadanlıqlara icazəsiz girişin qarşısını almaq üçün hasarlar, divarlar, barmaqlıqlar və maneələr kimi fiziki maneələrin istifadəsi daxildir.

Filtrasiya ehtimalını azaltmaq və CCTV sistemləri üçün görmə qabiliyyətini yaxşılaşdırmaq üçün bina və onların ətrafında yaxşı işıqlandırmanın təmin edilməsi daxildir. Maarifləndirməni artırmaq və sosial mühəndislik və digər hücumlar riskini azaltmaq üçün işçilərə fiziki təhlükəsizlik siyasətləri və prosedurları ilə bağlı təhsil və təlim keçirilməsi məqsədəuyğundur. Bütün bu tədbirlər birlikdə informasiya sisteminin fiziki mühafizəsinə kompleks yanaşmanı təmin edir və xarici və daxili hücumçular tərəfindən mümkün təhlükələrin qarşısını almağa kömək edir.

Texniki təhlükəsizlik – proqram təminatı və aparat vasitəsi ilə həyata keçirilən texniki və təhlükəsizlik tədbirlərini əhatə edir. Texniki təhlükəsizlik tədbirlərinə misal olaraq firewall, müdaxilənin aşkarlanması sistemləri (IDS), antivirus proqram təminatı, məlumatların şifrələnməsi, autentifikasiya və girişə nəzarət mexanizmlərinin istifadəsi və s. Texniki təhlükəsizliyin əsas elementləri aşağıdakılardır:

- Firewalllar.
- Müdaxilənin aşkarlanması sistemləri (IDS).
- Müdaxilənin qarşısının alınması Sistemləri (IPS).
- Antivirus proqramı.
- Monitorinq və hadisələrin qeydiyyatı.
- Məlumatların şifrələnməsi.
- Doğrulama mexanizmləri.
- Təhlükəsiz şəbəkə protokolları və xidmətləri.

Firewalllar şəbəkələr arasında trafikə nəzarət edən və süzgəcdən keçirən, icazəsiz qoşulmalardan və kənar hücumlardan qoruyan qurğular və ya proqramlardır. Hücumun aşkarlanması sistemləri (IDS) şəbəkə trafikinə nəzarət edir və onu müdaxilə əlamətləri və ya anomal davranış, hücumlar və ya təhlükəsizlik insidentləri barədə xəbərdar etmək üçün təhlil edir. Müdaxilənin qarşısının alınması Sistemləri (IPS) aşkar edilmiş təhdidlərə əsaslanaraq, əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydaları əsasında hücumları bloklayır və ya qarşısını alır. Bunlar viruslar, qurdlar, Trojan atları və digər zərərli proqramlar üçün sistemləri skan edən və onları silən və ya karantinə alan proqramlardır. Məlumatların Şifrələnməsi şəbəkə üzərindən ötürülən və ya cihazlarda saxlanılan məlumatların məxfiliyini qorumaq üçün kriptoqrafik üsullardan istifadə daxildir. Bunlar istifadəçilərin və cihazların autentifikasiyası üsullarıdır, məsələn, parollar, biometrik məlumatlar, aparat açarları və s.

Monitorinq sistemləri anomaliyaları aşkar etmək, insidentləri araşdırmaq və təhlükəsizlik qaydalarına riayət olunmasını təmin etmək üçün istifadəçi fəaliyyətlərini və hadisələri informasiya sistemində qeyd edir. Təhlükəsiz şəbəkə protokolları və xidmətləri təhlükəsiz məlumat ötürülməsi, autentifikasiya və məxfiliyi təmin edən şəbəkə səviyyəsi protokolları və xidmətlərindən istifadə daxildir. Bu texniki təhlükəsizlik elementləri informasiya resurslarının müxtəlif təhlükələrdən, o cümlədən zərərli proqramlardan, xarici hücumlardan və daxili təhlükəsizlik pozuntularından hərtərəfli qorunmasını təmin etmək üçün bir-biri ilə qarşılıqlı əlaqədə olur.

İnzibati təhlükəsizlik təşkilat daxilində təhlükəsizlik siyasətlərinin, prosedurlarının və təcrübələrinin idarə edilməsi və təşkili ilə məşğul olur. Buraya təhlükəsiz giriş siyasətlərinin işlənib hazırlanması, işçilərin informasiya təhlükəsizliyi üzrə təlimi, istifadəçi hesablarının idarə edilməsi, təhlükəsizlik auditinin aparılması və s. daxildir. Şəbəkə təhlükəsizliyinin bu növlərinin hər biri informasiya sisteminin qorunması üçün vacibdir və adətən hərtərəfli və etibarlı təhlükəsizlik sistemi yaratmaq üçün birlikdə istifadə olunur. İnzibati

təhlükəsizlik təşkilat daxilində təhlükəsizliyin idarə edilməsi üçün siyasətləri, prosedurları və təcrübələri əhatə edir. İnzibati təhlükəsizliyin əsas elementləri bunlardır:

- Təhlükəsizlik siyasəti.
- Prosedurlar və təlimatlar.
- Təhsil və maarifləndirmə.
- Giriş və imtiyazların idarə edilməsi.
- Audit və Monitorinq.
- Zəifliklərin idarə edilməsi.
- Risklərin idarə edilməsi.

İnformasiya resurslarının həyat dövrünün idarə edilməsi.

Təhlükəsizlik siyasəti – informasiya resurslarının təhlükəsizliyinə dair tələbləri və gözləntiləri müəyyən edən qaydaların, standartların və təlimatların müəyyən edilməsi. Təhlükəsizlik siyasətləri sənədləşdirilməli, işçilər üçün başa düşülməli və dəyişən təhlükə mühitini əks etdirmək üçün mütəmadi olaraq yenilənməlidir.

Prosedurlar və təlimatlar–Təhlükəsizlik siyasətlərini həyata keçirmək üçün tələb olunan xüsusi addımları və hərəkətləri müəyyən edən prosedurlar və təlimatlar hazırlanmalıdır. Buraya istifadəçinin qeydiyyatı, girişə nəzarət, zəifliyin idarə edilməsi, təhlükəsizlik insidentlərinin idarə edilməsi və s. prosedurları daxil ola bilər.

Təhsil və maarifləndirmə – Sistemlərdən istifadə, təhlükəsizlik təhdidləri, insidentlərə cavab prosedurları və s. daxil olmaqla, informasiya təhlükəsizliyi məsələləri ilə bağlı işçilərə təhsil və təlim vermək. İşçilərin təhlükəsizlikdən xəbərdar olmasını təmin etmək insan səhvi riskini azaltmağa və sistemin təhlükəsizliyini yaxşılaşdırmağa kömək edir.

Giriş və imtiyazların idarə edilməsi – İstifadəçilərin işinə olan ehtiyac əsasında informasiya resurslarına çıxışını tənzimləmək (ən az imtiyaz prinsipi), həmçinin sui-istifadə hallarının qarşısını almaq üçün sistem administratorlarının imtiyazlarına nəzarət etmək məqsədəuyğundur.

Audit və Monitorinq – Təhlükəsizlik siyasətlərinə uyğunluğu yoxlamaq, anomaliyaları müəyyən etmək və təhlükəsizlik insidentlərinin erkən aşkarlanması üçün istifadəçi fəaliyyətinə nəzarət etmək üçün müntəzəm sistem auditləri aparılması məqsədəuyğundur.

Zəifliklərin idarə edilməsi – Yamaqların, yeniləmələrin quraşdırılması və zəifliklərin müntəzəm skan edilməsi daxil olmaqla, informasiya sistemlərində

zəiflikləri aşkar etmək, qiymətləndirmək və azaltmaq üçün strategiyalar hazırlayın və həyata keçirir.

Risklərin idarə edilməsi – İnformasiya resurslarının təhlükəsizlik risklərinin təhlili və qiymətləndirilməsi, onların idarə edilməsi və azaldılması strategiyalarının hazırlanması, o cümlədən fövqəladə hallara və təhlükəsizlik insidentlərinə cavab tədbirlərinin planlaşdırılmasını həyata keçirir.

İnformasiya resurslarının həyat dövrünün idarə edilməsi – buraya informasiya ehtiyatlarının həyat dövrünün hər bir mərhələsində təhlükəsizlik tələbləri nəzərə alınmaqla onların yaradılması, istifadəsi, dəyişdirilməsi və silinməsi proseslərinin idarə edilməsi daxildir.

Bu inzibati təhlükəsizlik elementləri təşkilat daxilində effektiv təhlükəsizlik idarəçiliyini təmin etmək və qanunvericiliyə və təhlükəsizlik standartlarına uyğunluğu təmin etmək üçün əsasdır.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ ÜÇÜN ALƏTLƏR

Şəbəkə təhlükəsizliyi alətləri dedikdə adətən kompüter şəbəkələrini təhdidlərdən, hücumlardan və icazəsiz girişdən qorumaq üçün istifadə olunan müxtəlif vasitələr, texnologiyalar və metodlar başa düşülür. Şəbəkə təhlükəsizliyi alətləri şəkil 5.1-də təsvir olunmuşdur.

Şəkil 5.1. Şəbəkə təhlükəsizliyi alətləri

Şəkildən göründüyü kimi, alətlər Firewall, VPN, müdaxilənin qarşısının

alınması, davranışların təhlili daxildir. Firewall kənardan icazəsiz girişin və ya

hücumların qarşısını almaq üçün şəbəkənin müxtəlif seqmentləri arasında və ya şəbəkə ilə xarici şəbəkələr arasında trafiki izləyən və filtrləyən cihaz və ya proqramdır. VPN (Virtual Şəxsi Şəbəkə) İnternet kimi ictimai şəbəkələr üzərindən cihazlar arasında təhlükəsiz və şifrəli əlaqə təmin edən texnologiyadır. VPN məlumatların məxfiliyini qorumaq və məlumatın təhlükəsiz ötürülməsini təmin etmək üçün istifadə olunur. Intrusion Prevention Systems (IPS) zərərli və ya anomal davranış üçün şəbəkə trafikini təhlil edir və hücumların qarşısını almaq və ya qarşısını almaq üçün tədbirlər görür. Davranış Analizi istifadəçilərin və sistemlərin şəbəkədəki normal davranışını təhlil edir və trafik nümunələrində qəfil dəyişikliklər və ya təcavüzkar proqram fəaliyyəti kimi potensial təhlükəsizlik təhdidlərini göstərə bilən anomaliyaları aşkar edir. Bu alətlər şəbəkə təhlükəsizliyinin əsas komponentləridir və müxtəlif təhdidlərə və hücumlara qarşı tam şəbəkə qorunmasını təmin etmək üçün çox vaxt birlikdə istifadə olunur.

ƏN YAXŞI ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ SERTİFİKATLARI

Ən yaxşı şəbəkə təhlükəsizliyi[31] sertifikatlarının seçilməsi məqsədlərinizdən, təcrübə səviyyənizdən və ixtisasınızdan asılıdır. Bu sahədə tanınmış sertifikatlara aşağıdakılar daxildir.

- Certified Information Systems Security Professional (CISSP).
- Certified Ethical Hacker (CEH).
- CompTIA Security+.
- Sertifikatlaşdırılmış İnformasiya Təhlükəsizliyi Meneceri (CISM).
- Cisco Certified CyberOps Associate.
- Sertifikatlaşdırılmış İnformasiya Təhlükəsizliyi Auditoru (CISA).

CISSP informasiya təhlükəsizliyi sahəsində ən hörmətli sertifikatlardan biridir. O, sistemlərə giriş, kriptoqrafiya, şəbəkə təhlükəsizliyi, risklərin idarə edilməsi və s. daxil olmaqla geniş mövzuları əhatə edir. CEH, sistemlərini daha yaxşı qorumaq üçün hakerlərin hücum üsullarını anlamaq istəyən peşəkarlar üçündür. Bu sertifikat həm də nüfuz testində iştirak edən təhlükəsizlik

[31] Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.
Rzayeva G., İbrahimova A. Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi. Dərs vəsaiti. Bakı: "Nurlar" nəşriyyatı, 2021, 200 s.

mütəxəssisləri üçün faydalı ola bilər. informasiya təhlükəsizliyi üzrə peşəkarlar üçün sertifikatdır. O, şəbəkələri, tətbiqləri və məlumatları qorumaq üçün lazım olan əsas anlayışları və bacarıqları əhatə edir. CompTIA Security+ sertifikat informasiya təhlükəsizliyinin idarə edilməsi sahəsində çalışan peşəkarlar üçün nəzərdə tutulub. O, informasiya təhlükəsizliyinin idarəetmə aspektlərini, o cümlədən strateji planlaşdırma, risklərin idarə edilməsi və təhlükəsizlik proqramının idarə edilməsini əhatə edir. Sertifikatlaşdırılmış İnformasiya Təhlükəsizliyi Meneceri (CISM) sertifikat Cisco məhsulları ilə işləyən təhlükəsizlik mütəxəssisləri üçün nəzərdə tutulub. O, təhlükəsizlik monitorinqi, hücumun aşkarlanması və insidentlərə reaksiya kimi mövzuları əhatə edir. Cisco Certified CyberOps Associate sertifikat sistemləri və prosesləri təhlükəsizlik standartlarına və normativ tələblərə uyğunluğu yoxlayan informasiya təhlükəsizliyi auditorları üçündür. Sertifikatlaşdırılmış İnformasiya Təhlükəsizliyi Auditoru (CISA) unlar şəbəkə təhlükəsizliyi sahəsində ən tanınmış və tanınmış sertifikatlardan yalnız bəziləridir. Karyera məqsədlərinizə və ixtisasınıza ən uyğun olan sertifikatı seçmək vacibdir. Şəbəkə təhlükəsizliyi sahəsində böyük pullar qazanmazdan əvvəl alətləri və bacarıqları öyrənməlisiniz. Şəbəkə təhlükəsizliyi üzrə təlimlər burada işə düşür. Şəbəkə təhlükəsizliyi üzrə sertifikatlaşdırma kursları sizə bu vəzifələr üçün vacib biliklər verməklə yanaşı, həm də potensial işəgötürənlərə tələb olunan keyfiyyətlərə malik olduğunuzu göstərən qiymətli sertifikat verir.

İT İNFRASTRUKTURUNUN YARADILMASI PRİNSİPLƏRİ

Son bir neçə onillikdə informasiya təhlükəsizliyi tələbləri əhəmiyyətli dərəcədə dəyişib. Məlumatların avtomatlaşdırılmış emalı sistemlərinin geniş tətbiqindən əvvəl informasiya təhlükəsizliyi yalnız fiziki və inzibati tədbirlərlə təmin edilirdi. Kompüterlərin meydana gəlməsi ilə məlumat fayllarını və proqram mühitini qorumaq üçün avtomatik vasitələrdən istifadə ehtiyacı aydın oldu. Avtomatik təhlükəsizlik vasitələrinin inkişafının növbəti mərhələsi paylanmış məlumatların emalı sistemlərinin və kompüter şəbəkələrinin yaranması ilə bağlıdır ki, bu zaman şəbəkə təhlükəsizlik vasitələrindən faylları və proqram mühitini qorumaqla yanaşı, şəbəkələr vasitəsilə ötürülən məlumatların mühafizəsi üçün istifadə edilməlidir. Ən dolğun təfsirdə, şəbəkə təhlükəsizliyi tədbirləri dedikdə, məlumatların şəbəkələr üzərindən ötürülməsi zamanı baş verən təhlükəsizlik pozuntularının qarşısının alınması tədbirləri,

habelə bu cür təhlükəsizlik pozuntularının baş verdiyini müəyyən etmək üçün tədbirlər nəzərdə tutulur.

Kompüter şəbəkələrindən istifadə zamanı yaranan tipik təhlükəsizlik problemləri aşağıdakılardır:

1. Şirkətin bir-birindən kifayət qədər böyük məsafədə yerləşən bir neçə ofisi var. Ümumi şəbəkə (məsələn, İnternet) üzərindən məxfi məlumatları göndərərkən, heç kimin bu məlumatı casusluq edə və ya dəyişdirə bilməyəcəyinə əmin olmalısınız.

2. Şəbəkə administratoru kompüteri uzaqdan idarə edir. Düşmən istifadəçi nəzarət mesajını ələ keçirir, məzmununu dəyişdirir və mesajı hədəf kompüterə göndərir.

3. İstifadəçi qanuni istifadəçinin hüquqları ilə uzaq kompüterə icazəsiz giriş əldə edir və ya kompüterə daxil olmaq hüququna malik olmaqla daha böyük hüquqlarla çıxış əldə edir.

4. Şirkət ödənişləri elektron şəkildə qəbul edən onlayn mağaza açır. Bu halda satıcı əmin olmalıdır ki, həqiqətən pulu ödənilmiş məhsulu buraxır və alıcının birincisi, ödənişli məhsulu alacağına, ikincisi, kredit kartı nömrəsinin məlum olmayacağına zəmanət olmalıdır. kiməsə.

5. Şirkət internetdə öz internet saytını açır. Müəyyən bir məqamda saytın məzmunu yenisi ilə əvəz olunur və ya belə bir axın və sayta daxil olmaq üçün elə bir üsul yaranır ki, server sorğuların işlənməsinin öhdəsindən gələ bilmir. Nəticədə, adi veb-sayt ziyarətçiləri ya şirkətlə heç bir əlaqəsi olmayan məlumatları görürlər, ya da sadəcə olaraq şirkətin veb saytına daxil ola bilmirlər.

İnformasiya təhlükəsizliyi ilə bağlı əsas anlayışlara və onların əlaqəsinə baxaq. Sahib, müxtəlif növ hücumlardan qorunmalı olan bir sıra məlumat dəyərlərini (aktivlərini) müəyyənləşdirir. Hücumlar qorunan aktivlərdə müxtəlif zəifliklərdən istifadə edən təhdid agentləri və ya rəqiblər tərəfindən həyata keçirilir. Əsas təhlükəsizlik pozuntuları informasiya aktivlərinin açıqlanması (məxfiliyin itirilməsi), onların icazəsiz dəyişdirilməsi (bütövlüyün itirilməsi) və ya bu aktivlərə icazəsiz girişin itirilməsi (mövcudluğun itirilməsi) olur.

İnformasiya aktivlərinin sahibləri qorunan resursların zəifliklərini və müəyyən mühitdə baş verə biləcək mümkün hücumları təhlil edirlər. Bu təhlil nəticəsində müəyyən informasiya aktivləri üçün risklər müəyyən edilir. Bu təhlil təhlükəsizlik siyasəti ilə müəyyən edilən və təhlükəsizlik mexanizmləri və xidmətləri vasitəsilə həyata keçirilən əks tədbirlərin seçimini müəyyənləşdirir.

Nəzərə almaq lazımdır ki, fərdi zəifliklər hətta təhlükəsizlik mexanizmləri və xidmətlərinin tətbiqindən sonra da davam edə bilər. Təhlükəsizlik siyasəti qorunan aktivlərə və onların istifadə olunduğu mühitə adekvat olan ardıcıl təhlükəsizlik mexanizmləri və xidmətlərini müəyyən edir. Şəbəkə təhlükəsizliyinin inkişafında istifadə olunan əsas terminlərə aşağıdakılar daxildir:

Zəiflik – sistemdə hücum etmək üçün istifadə edilə bilən zəif nöqtədir. Risk, müəyyən bir zəiflikdən istifadə edərək konkret hücumun həyata keçirilmə ehtimalıdır. Nəhayət, hər bir təşkilat dözə biləcəyi risk səviyyəsinə qərar verməlidir. Bu qərar təşkilatın qəbul etdiyi təhlükəsizlik siyasətində öz əksini tapmalıdır.

Təhlükəsizlik siyasəti – informasiya aktivlərinin təşkilat daxilində və informasiya sistemləri arasında necə emal edildiyini, mühafizəsini və paylanmasını müəyyən edən qaydalar, təlimatlar və təcrübələr; təhlükəsizlik xidmətlərinin göstərilməsi üçün bir sıra meyarlar.

Hücum – informasiya sisteminin təhlükəsizliyini pozan hər hansı bir hərəkətdir. Daha formal olaraq deyə bilərik ki, hücum müəyyən bir informasiya sisteminin zəifliklərindən istifadə edən və təhlükəsizlik siyasətinin pozulmasına səbəb olan hərəkət və ya bir-biri ilə əlaqəli hərəkətlər ardıcıllığıdır.

Təhlükəsizlik mexanizmi – hücumu aşkarlayan və/və ya qarşısını alan proqram və/yaxud aparat cihazıdır.

Təhlükəsizlik xidməti – sistemlərin və/yaxud ötürülən məlumatların siyasətlə müəyyən edilmiş təhlükəsizliyini təmin edən və ya hücumun həyata keçirilməsini müəyyən edən xidmətdir. Xidmət bir və ya bir neçə təhlükəsizlik mexanizmindən istifadə edir.

Əsas prinsip ondan ibarətdir ki, İT xidmətlərinin həyat qabiliyyətinin təmin edilməsi, nasazlıqların və müdaxilələrin minimuma endirilməsi müxtəlif texnologiyaların inteqrasiyası yolu ilə həyata keçirilməlidir. Dərin müdafiə dedikdə, uğursuzluqların və nüfuzların minimuma endirilməsi üçün bir-biri ilə əlaqəli bir neçə texnologiyanın istifadə olunduğu informasiya infrastrukturunun yaradılması nəzərdə tutulur. Dərin müdafiə yaradılarkən İT xidmətlərinin etibarlılığı və elastikliyi təmin edilir. İT sistemlərinin hücumlara müqavimət göstərmə qabiliyyəti, onların xidmətlərə təsirini minimuma endirməkdir. Təhlükəsizliyi təmin etmək üçün əlçatanlığı, bütövlüyünü, autentifikasiyasını, məxfiliyini və rədd edilməməsini təmin etməklə informasiya sistemlərini qoruyan mexanizmləri müəyyən etmək lazımdır.

ŞƏBƏKƏ PERİMETRİNİN TƏHLÜKƏSİZLİYİNİN QURULMASI METODOLOGİYASI

Şəbəkə perimetri daxili şəbəkə resursları ilə İnternet və ya üçüncü tərəf şəbəkələri kimi xarici mənbələr arasındakı sərhədi və ya sərhədi ifadə edir. Bu konsepsiya məlumatların və trafikin təşkilatın daxili şəbəkəsi ilə xarici dünya arasında hərəkət etdiyi bütün nöqtələri əhatə edir. Şəbəkənin perimetrində müxtəlif təhlükəsizlik və girişə nəzarət mexanizmləri quraşdırılmışdır. Firewall və müdaxilə aşkarlama sistemləri kimi bu cihaz və sistemlər icazəsiz giriş və hücumların qarşısını almaq üçün trafiki süzmək və izləmək üçün nəzərdə tutulub. Onlar şəbəkəyə daxil olan və çıxan trafiki təhlil edir və idarə edir, daxili resursları potensial təhlükələrdən qoruyur və məlumatların təhlükəsizliyini təmin edir. Şəbəkə perimetri məlumatların məxfiliyinin və bütövlüyünün təmin edilməsində də mühüm rol oynayır. O, şifrələmə və digər təhlükəsizlik texnologiyalarından istifadə etməklə, xarici mənbələrlə qarşılıqlı əlaqədə olarkən məlumatların necə ötürüldüyünə və işlənməsinə nəzarət edir. Bu, məlumat sızmasının qarşısını almağa və onları təhlükəsiz saxlamağa kömək edir. Şəbəkə perimetrinin mühüm aspekti şəbəkə performansını optimallaşdırmağa və şəbəkə sıxlığının qarşısını almağa kömək edən trafikin idarə edilməsidir. Buraya bant genişliyinə nəzarət və müxtəlif trafik növlərinin prioritetləşdirilməsi daxildir. Şəbəkə perimetri həmçinin viruslar və zərərli proqramlar kimi xarici təhlükələrdən qorunma təmin edir. Perimetrdə istifadə olunan texnologiyalar və həllər potensial təhlükəli hücumların aşkarlanması və bloklanması, onların şəbəkəyə nüfuz etməsinin qarşısının alınması məqsədi daşıyır.

Beləliklə, şəbəkə perimetri təhlükəsizlik strategiyasında əsas rol oynayır, hansı məlumatların və trafikin şəbəkəyə daxil olub çıxa biləcəyini müəyyənləşdirir və daxili resursların xarici təhlükələrdən qorunmasını təmin edir. Şəbəkə perimetri təhlükəsizliyinin yaradılması metodologiyası şəbəkənin xarici sərhədlərini təhdid və hücumlardan qorumağa yönəlmiş bir sıra addımlar və strategiyaları əhatə edir. Bu metodologiyaya aşağıdakıları əhatə edir:

- Zəifliyin qiymətləndirilməsi.
- Aktivlərin və resursların identifikasiyası.
- Təhlükəsizlik strategiyasının hazırlanması.
- Təhlükəsizlik strategiyasının hazırlanması.
- Təhlükəsizlik tədbirlərinin tətbiqi.

- Monitorinq və təhlil.
- İnsidentə cavab.
- Audit və yeniləmə.

Şəbəkə perimetrinin təhlükəsizliyinin təmin edilməsi metodologiyası zəifliyin qiymətləndirilməsi ilə başlayır ki, bu da infrastrukturun zəif nöqtələrini və təcavüzkarlar üçün mümkün giriş nöqtələrini müəyyən etməyə imkan verir. Bu qiymətləndirməyə potensial təhdidlərin təhlili, şəbəkə cihazı konfiqurasiyalarının nəzərdən keçirilməsi və mövcud təhlükəsizlik tədbirlərinin qiymətləndirilməsi daxildir. Əldə edilmiş məlumatlar əsasında perimetrin gücləndirilməsinə və müəyyən edilmiş zəifliklərin aradan qaldırılmasına yönəlmiş təhlükəsizlik strategiyası hazırlanır.

Növbəti addım hansı cihazların və məlumatların qorunmağa ehtiyacı olduğunu müəyyən etməyə imkan verən aktivlərin və resursların müəyyənləşdirilməsidir. Bu məlumat səylərinizi serverlər, verilənlər bazaları və əsas proqramlar kimi şəbəkənizin ən kritik elementlərinə cəmləməyə kömək edir. Daha sonra təhlükəsizlik strategiyası işlənib hazırlanır və həyata keçirilir ki, bura perimetri qorumaq üçün müvafiq texnologiyalar və metodların seçilməsi daxildir.

Təhlükəsizlik tədbirlərinin həyata keçirilməsinə təhlükəsizlik divarları, müdaxilənin aşkarlanması sistemləri və antivirus proqram təminatı kimi təhlükəsizlik sistemlərinin konfiqurasiyası və yerləşdirilməsi daxildir. Bu tədbirlər trafiki izləməyə və filtrləməyə, icazəsiz giriş və hücumların qarşısını almağa kömək edir. Bununla paralel olaraq anomaliyaları və potensial təhlükələri tez müəyyən etmək üçün şəbəkə trafikinin monitorinqinin və təhlilinin qurulması vacibdir.

Təhlükəsizliyin qorunmasında əsas rolu insidentlərə cavab verir, çünki təhlükələrin vaxtında aşkarlanması və aradan qaldırılması zərəri minimuma endirməyə kömək edir. Normal şəbəkə fəaliyyətini tez bir zamanda bərpa etmək və təkrar hücumların qarşısını almaq üçün insidentlərə operativ reaksiya vermək üçün aydın fəaliyyət planının olması vacibdir.

Təhlükəsizlik tədbirlərinin müntəzəm yoxlanılması və yenilənməsi mühafizənizin yeni və effektiv olmasını təmin edir. Audit sizə təhlükəsizlik sisteminizin cari vəziyyətini qiymətləndirməyə və dəyişikliklərə ehtiyacı müəyyən etməyə imkan verir və təhlükəsizlik tədbirlərinin yenilənməsi onları yeni təhdidlərə və zəifliklərə uyğunlaşdırmağa kömək edir.

Beləliklə, şəbəkə perimetri təhlükəsizliyinin təmin edilməsi metodologiyasına risklərin qiymətləndirilməsi, mühafizə strategiyasının

işlənib hazırlanması və həyata keçirilməsi, təhlükəsizlik vəziyyətinin monitorinqi, insidentlərə operativ reaksiya verilməsi və mühafizə tədbirlərinin mütəmadi olaraq yenilənməsinə yönəlmiş kompleks yanaşma daxildir.

YOXLAMA SUALLARI

1. Şəbəkə təhlükəsizliyinin əsas məqsədləri hansılardır və onlar təşkilat üçün nə üçün vacibdir?
2. Şəbəkə infrastrukturunun hansı aspektləri şəbəkə təhlükəsizliyinin əhatə dairəsinə düşür?
3. Bir təşkilatda şəbəkə təhlükəsizliyi üzrə mütəxəssisin vəzifə və öhdəlikləri hansılardır?
4. Şəbəkə təhlükəsizliyinə təsir edə biləcək müxtəlif təhdid növləri hansılardır?
5. Şəbəkə hücumlarının hansı növləri mövcuddur və onları necə təsnif etmək olar?
6. Şəbəkə təhlükəsizliyini təmin etmək üçün hansı alətlər və texnologiyalardan istifadə olunur?
7. Firewall, müdaxilənin aşkarlanması sistemləri və antivirus proqramları kimi alətlərin işinin əsasında hansı prinsiplər dayanır?
8. Şəbəkə təhlükəsizliyi mütəxəssisləri üçün hansı sertifikatlaşdırma proqramları var?
9. Karyera yüksəlişi üçün şəbəkə təhlükəsizliyi sertifikatının alınmasının əhəmiyyəti və faydaları nədir?
10. Təhlükəsiz şəbəkə infrastrukturunun layihələndirilməsi zamanı nəzərə alınmalı əsas prinsiplər hansılardır?
11. Şəbəkə infrastrukturunuzdakı zəiflikləri və riskləri minimuma endirmək üçün hansı addımları ata bilərsiniz?
12. Şəbəkə perimetrinin təhlükəsizliyini təmin etmək üçün hansı üsul və yanaşmalardan istifadə olunur?
13. Şəbəkə perimetri təhlükəsizliyinin qurulması üçün əsas addımlar hansılardır?

PRAKTİKİ TAPŞIRIQ

1. Şəbəkə infrastrukturunun təhlükəsizlik səviyyəsinin qiymətləndirilməsi.

Tapşırıq: Təhlükəsizliyin mövcud səviyyəsini qiymətləndirmək üçün şəbəkə infrastrukturunun auditini aparın. Təhlilinizə zəifliklərin olması və firewall və müdaxilə aşkarlama sistemlərinin düzgün konfiqurasiya edilib-edilməməsi kimi amilləri daxil edin.

Məqsəd: Potensial şəbəkə təhlükəsizliyi zəifliklərini və zəifliklərini müəyyən etmək və onların aradan qaldırılması üçün plan hazırlamaq.

2. Təşkilatın təhlükəsizlik siyasətinin inkişafı.

Tapşırıq: Şəbəkədən istifadə, resurslara daxil olmaq, məxfi məlumatların mühafizəsi və s. standartlarını və qaydalarını müəyyən edən təhlükəsizlik siyasəti sənədi yaradın.

Məqsəd: Təşkilatda vahid təhlükəsizlik standartlarını təmin etmək və bütün işçilər tərəfindən riayət edilməli olan qaydaları formalaşdırmaq.

3. Şəbəkə təhlükəsizliyi üçün təhdidlərin və risklərin təhlili.

Tapşırıq: Təşkilatınızın şəbəkə təhlükəsizliyinə təsir edə biləcək təhdid və risklərin təhlilini aparın. Ən çox ehtimal olunan təhlükələri müəyyənləşdirin və onların potensial təsirini qiymətləndirin.

Məqsəd: Təhdidlərin və risklərin şəbəkə infrastrukturuna təsirini minimuma endirməyə yönəlmiş təhlükəsizlik strategiyasının hazırlanması.

4. Firewallların və müdaxilənin aşkarlanması sistemlərinin konfiqurasiyası.

Tapşırıq: Şəbəkə infrastrukturunu xarici hücumlardan və daxili təhdidlərdən qorumaq üçün firewallları və müdaxilənin aşkarlanması sistemlərini (IDS/IPS) konfiqurasiya edin.

Məqsəd: Təhlükəsizlik mexanizmlərinin optimal səviyyədə işləməsini təmin etmək və şəbəkəyə uğurlu hücumlar ehtimalını azaltmaq.

5. İşçilər üçün təhlükəsizlik üzrə maarifləndirmə və təlimlərin keçirilməsi.

Tapşırıq: İnformasiya təhlükəsizliyi məsələləri, o cümlədən təhlükəsiz onlayn davranış prinsipləri, fişinq hücumlarının tanınması və s. üzrə işçilər üçün təlim tədbirləri təşkil edin.

Məqsəd: İşçilərin şəbəkə təhlükəsizliyi haqqında məlumatlılığını artırmaq və diqqətsiz davranış nəticəsində daxili təhdidlər riskini azaltmaq.

6. Bank sektoru.

Tapşırıq: Müştəri hesablarını icazəsiz girişdən qorumaq üçün onlayn bankçılıq üçün iki faktorlu autentifikasiya sistemini hazırlayın və tətbiq edin.

Məqsəd: Müştərilərin maliyyə əməliyyatları üçün əlavə təhlükəsizlik səviyyəsini təmin etmək və onları şəxsi məlumatların oğurlanmasından qorumaq.

7. Təhsil.

Məqsəd: Tələbələr və təhsil müəssisəsinin işçiləri üçün informasiya təhlükəsizliyi üzrə təlim kursları, o cümlədən şəxsi məlumatların qorunması və sosial mühəndisliyin tanınması üzrə sessiyalar keçirmək.

Məqsəd: İştirakçıların ümumi təhdidlər və təhsil mühitində şəxsi məlumatların qorunması üsulları haqqında məlumatlılığını artırmaq.

8. Səhiyyə.

Məqsəd: Məxfilik və məlumatların bütövlüyü tələblərini nəzərə alaraq, HIPAA standartlarına uyğun olaraq tibbi məlumatlara girişin idarə edilməsi sistemini hazırlamaq və həyata keçirmək.

Məqsəd: Xəstənin tibbi məlumatlarının təhlükəsizliyini təmin etmək və onlara ica zəsiz girişin qarşısını almaq.

9. Hərbi.

Məqsəd: Hərbi personala kibertəhlükəsizlik təlimi, o cümlədən kiberhücum simulyasiyaları və fişinq hücumlarının tanınması və qarşısının alınması üzrə təlimlər verməkk.

Məqsəd: Kibertəhlükələri idarə etmək və hərbi informasiya infrastrukturunun təhlükəsizliyini təmin etmək üçün şəxsi heyətin hazırlanması.

10. Onlayn ticarət.

Tapşırıq: İstifadəçi davranışını təhlil etmək və şübhəli əməliyyatları müəyyən etmək üçün maşın öyrənmə alqoritmlərindən istifadə edərək onlayn mağaza üçün fırıldaqçılığın aşkarlanması sistemini hazırlayın və tətbiq edin.

Məqsəd: Fırıldaqçılıq nəticəsində maliyyə itkiləri riskini azaltmaq və müştəri ödəniş məlumatlarının təhlükəsizliyini təmin etmək.

MODUL 6. SİMSİZ (Wİ-Fİ) TƏHLÜKƏSİZLİK

SİMSİZ (Wİ-Fİ) TEXNOLOGİYALARIN ƏSASLARI
SİMSİZ TEXNOLOGİYANIN ƏSAS KOMPONENTLƏRİ VƏ PROTOKOLLARI
KRİPTOQRAFİYA VƏ ŞİFRƏLƏMƏ PROTOKOLLARI
MAC ÜNVAN FİLTRLƏMƏ
CİHAZIN YERLƏŞDİRİLMƏSİ QAYDASI VƏ SİQNAL GÜCÜ

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

SİMSİZ (Wİ-Fİ) TEXNOLOGİYALARIN ƏSASLARI

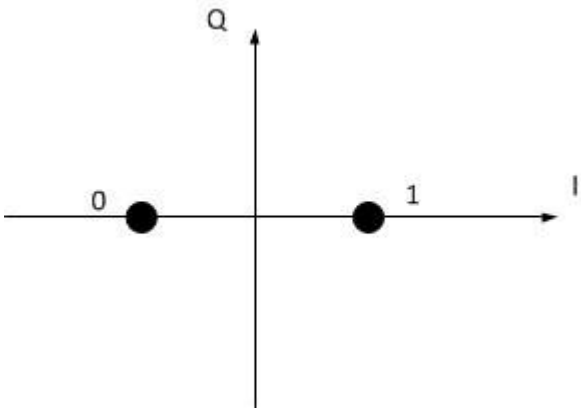
Simsiz rabitə vəziyyətində məlumat ötürülməsi radio havasındakı elektromaqnit dalğaları vasitəsilə baş verir. Simsiz rabitə üçün 300 - 3000 MHz diapazonunda və 1-10 dm dalğa uzunluğunda ultra yüksək tezlikli əraziyə (UHF - Ultra Yüksək Tezliklər) uzanan tezliklər istifadə olunur. Bu, cib telefonlarının, simsiz rabitə cihazlarının, televiziya ötürücülərinin və mikrodalğalı sobaların işlədiyi desimetr dalğaları bölgəsidir. Məlumat ötürmək üçün daşıyıcı siqnallar modulyasiya edilir. Modulyasiya üsullarına aşağıdakılar daxildir:

- Daşıyıcı siqnalın amplitudasının məlumat siqnallarına uyğun olaraq dəyişdirildiyi amplituda modulyasiyası (AM).

- Daşıyıcı siqnalın tezliyinin məlumat siqnallarına uyğun olaraq dəyişdirildiyi tezlik modulyasiyası (FM).

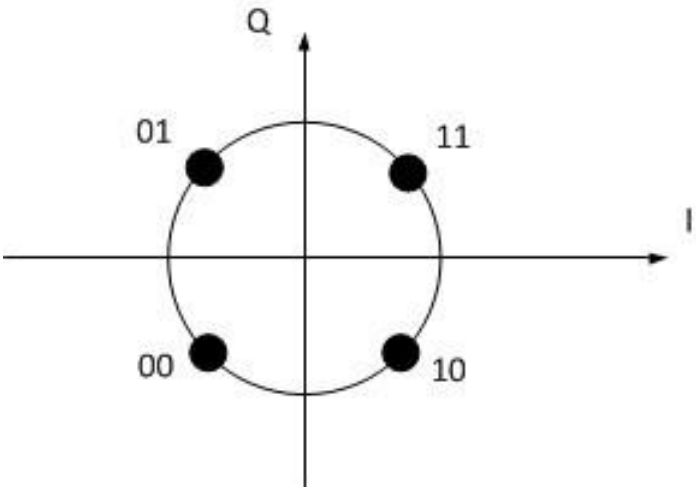
- Faza modulyasiyası (PM), daşıyıcı siqnalın fazasının ötürülən məlumat siqnallarına uyğun olaraq dəyişdiyi modulyasiya.

Rəqəmsal faza modulyasiyası (PSK - Phase-Shift Anahtaring) faza modulyasiya üsuludur, onun ən sadə variantı ikili faza modulyasiyasıdır, burada ötürücü dalğanın fazasının yalnız 2 mümkün dəyəri var: 0 və 180 dərəcə. İkili faza modulyasiyası vəziyyətində hər simvol bir bit ötürür (şəkil 6.1).



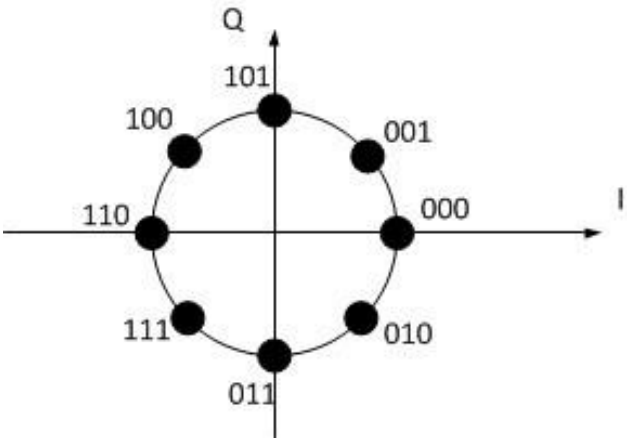
Şəkil 6.1 Binar faza modulyasiyası
(Q - kvadratura komponenti; I - fazadaxili komponent)

Kvadrat faza modulyasiyası vəziyyətində , ötürücü dalğanın fazası 90 dərəcə artımlarla 4 fərqli dəyərə malik ola bilər ki, bu da hər bir simvol ilə 2 bit ötürməyə imkan verir (şəkil 6.2).



Şəkil 6.2. Kvadrat faza modulyasiyası
(Q - quadratura komponenti; I - fazadaxili komponent)

8 fazalı faza modulyasiyası 8PSK də istifadə olunur ki, bu da hər simvolla 3 bit ötürməyə imkan verir. O, məsələn, EDGE məlumat ötürülməsi vəziyyətində istifadə olunur. Simvol başına 3 bit istifadə edərək, hər bir simvol 8 fərqli dəyər ötürə bilər. Bu yolla məlumat ötürmə sürətini artıra bilərsiniz (şəkil 6.3).



Şəkil 6.3. 8PSK faza modulyasiyası
(Q - quadratur komponenti; I - fazadaxili komponent)

Qəbul edən tərəfdə hansı fazanın hansı siqnal dəyərinə uyğun olduğunu müəyyən etmək üçün fazası məlum olan sinxronlaşdırılmış dəstək siqnalından istifadə etmək lazımdır. Buna görə də, diferensial faza modulyasiyası əsasən

rəqəmsal rabitə sistemlərində istifadə olunur, bu halda dəstək siqnalına ehtiyac yoxdur.

Diferensial modulyasiya ilə siqnal dəyişikliyinin əsasını əvvəlki dəyər təşkil edir, yəni xüsusi bitlərin əvvəlki dəyəri ilə fərqi nəzərə alınır. Diferensial iki fazalı keçid açarı (DBPSK) siqnalın fazasının çevrilməsindən istifadə edən modulyasiya sxemidir. 0 dəyəri dəyişməmiş fazaya uyğundur, 1 dəyəri isə fazanı dəyişir. Bu yanaşma, məsələn, siqnal ötürülməsi üçün WiFi şəbəkələrində istifadə olunur.

Diferensial Kvadrat Faza Köçürülməsi (DQPSK)- bu modulyasiya texnikası vəziyyətində faza 4 fərqli dəyərə malik ola bilər. 2 Mbit/s məlumat ötürülməsi ilə WiFi və ya Bluetooth şəbəkələrində istifadə olunur. 4 və ya daha çox biti ötürmək üçün dördüncü amplituda modulyasiyasından (QAM) istifadə olunur , burada fazaya əlavə olaraq daşıyıcı dalğanın amplitudası da modullaşdırılır. İki 90 dərəcə sürüşmə ilə bu modulyasiya vəziyyətində, daşıyıcı siqnalın amplitudası məlumat siqnalını təmsil etmək üçün dəyişdirilir, QAM modulyasiyası vəziyyətində, hər bir simvol ilə 2 bit ötürülə bilər: bir bit birinə uyğundur. ikinci bit daşıyıcı siqnalın digər amplitudasına. Hər bir daşıyıcı siqnal iki səviyyədə modelləşdirilirsə, onda biz DQPSK modulyasiyasını əldə edirik və dörd mümkün simvoldan biri bir anda ötürülə bilər - 4QAM. Müxtəlif QAM variasiyaları 16 ilə 256 arasında dəyişir. Nömrə nə qədər çox olarsa, məsafə bir o qədər qısa olar və düzgün ötürmə üçün bir o qədər az səs-küy olur.

Rəqəmsal ötürülmə ya dar zolaqlı ötürmə texnologiyasından istifadə etməklə, ya da spektral parçalanma üsullarından istifadə etməklə baş verə bilər.

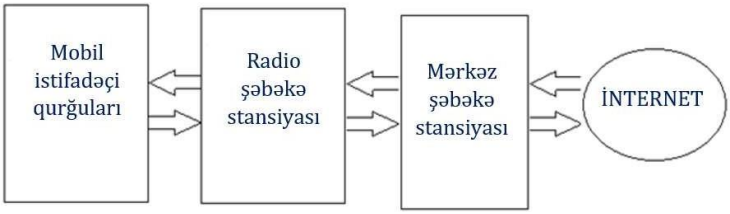
Texnologiya spektral parçalanmışdır və məlumat ötürülməsini mövcud bant genişliyinə bölür. Bu şəkildə daha çox səs-küyə qarşı müqavimət əldə edilir. Mobil rabitə və simsiz şəbəkələrdə istifadə olunur. Simsiz şəbəkələr aşağıdakı kimi təsnif olunur:

- GSM (Mobil rabitə üçün Qlobal Sistem).
- UMTS (Universal Mobile Telecommunications System).
- 4G.
- WLAN (Wireless Lan).
- Home RF.
- WPAN (Simsiz Şəxsi Sahə Şəbəkəsi).

GSM (Mobil Rabitə üçün Qlobal Sistem) ən populyar mobil mobil texnologiyadır. GSM, ötürücüləri, qəbulediciləri və antenaları özündə birləşdirən baza stansiyalarına (BTS - Base Transceiver Station) əsaslanan rabitə şəbəkəsini müəyyən edir. Baza stansiyaları sözdə idarə olunur. baza

stansiyası nəzarətçisi (BSC - Baza Stansiyası Nəzarətçisi). BSC-nin vəzifəsi bir baza stansiyasının əhatə dairəsindən zəncirdə növbəti stansiyanın əhatə dairəsinə keçməklə (zəruri hallarda) mobil telefonları birləşdirmək üçün kanalları idarə etmək və ayırmaqdır. Mobil şəbəkə mərkəzi stansiyası (MSC - Mobil Kommutasiya Mərkəzi) baza stansiyasının nəzarətçiləri ilə simli rabitə şəbəkəsi arasında əlaqəni idarə edir. GSM iki tezlikdən istifadə edir: 900 MHz və 1800 MHz. Baza stansiyalarının gücü təxminən 20 Vt, mobil telefonlar üçün isə 2 Vt təşkil edir. Mobil telefonlar (və ya terminallar) üçün siqnal gücü baza stansiyaları tərəfindən idarə olunur və müdaxilə etməmək üçün normal əlaqəni təmin edən minimuma endirilir. hüceyrədəki digər əlaqələr. GSM nitqi 13 kbit/s-dən yuxarı sürətlə ötürməyə imkan verən sıxılmış formatda nitq ötürür. Sıxılma texnikası RPELTP (Regular Pulse Excitation Long Term Predictor). Qoşularkən qonşu stansiyalar müxtəlif qonşu stansiyalara müxtəlif tezlikləri ayıran FDMA (Frequency Division Multiple Access) texnikasından istifadə edirlər. Əlaqələrə müdaxilənin qarşısını almaq üçün qəbul edilən və ötürülən siqnalların tezlikləri fərqlidir. Müxtəlif terminalların eyni vaxtda şəbəkədən istifadə etməsinə icazə vermək üçün TDMA (Time Division Multiple Access) texnologiyası tətbiq edilir. Bu zaman əsas kanal müxtəlif söhbətlərə (əlaqələrə) uyğun gələn vaxt intervallarına bölünür və beləliklə, onların birgə ötürülməsi mümkün olur. İstinad stansiyaları və terminallar arasında istifadə olunan modulyasiya texnikası GSMK-dır. Rəqəmsal məlumat ötürmə texnologiyası GPRS boş vaxt boşluqlarından istifadə edir. GSM-in əsas məlumat ötürmə sürəti 9600 bit/s təşkil edir, lakin boş vaxt intervallarından istifadə etməklə sürəti 56 kbit/s-ə qədər artırmaq olar. Təkmilləşdirilmiş GSM rabitəsi (EDGE - GSM Evolution üçün Enhanced Data rates) GPRS texnologiyasının davamçısıdır və 384 kbit/s-ə qədər məlumat ötürmə sürətini təmin edir. Rabitə ilə yanaşı, multimedia proqramlarından da istifadə etməyə imkan verir. EDGE GSM texnologiyasını tamamlayır və eyni vaxt bölgüsü multipleksasiyası (TDMA) strukturundan və mövcud GSM şəbəkələrindən istifadə edir.

UMTS. Üçüncü nəsil mobil rabitə ilə məşğul olduğumuz üçün GSM sistemi indi 3G sistemi kimi tanınan UMTS sisteminə keçir. UMTS-in məntiqi strukturu mahiyyətcə GSM-ə bənzəyir. "B node" cihazlarına xidmət edən hüceyrələr (UTRAN - UMTS Terrastrial Radio Access Network) var ki, bu da öz növbəsində radio şəbəkə nəzarətçi stansiyası (RNC - Radio Network Controller) tərəfindən idarə olunur) simli rabitə şəbəkəsi və radio şəbəkə nəzarətçi stansiyası arasında əlaqə kanalı əlavə edir (şəkil 6.4).



Şəkil 6.4. UMTS şəbəkə arxitekturası

Mərkəzi stansiyanın bir hissəsi SGSN (Serving GPRS Support Node), funksiyası təhlükəsizliyi və girişə nəzarəti təmin etmək, həmçinin xarici IP şəbəkəsindən IP paketləri istiqamətləndirən GGSN (Gateway GPRS Support Node) təşkil edir. SGSN. Simli şəbəkədə UMTS ATM texnologiyasını, simsiz şəbəkədə isə genişzolaqlı CDMA texnologiyasını (WCDMA - Wideband Code-Division Multiple Access) tətbiq edir. WCDMA yerli şəbəkə və İnternetə aşağı güc və sürətli bağlantılardan istifadə edərək məlumat, səs və video ötürülməsini təklif edir. WCDMA vəziyyətində tezlik modulyasiyası naxışda modulyasiya edilmiş psevdo-təsadüfi radio siqnalı ilə həyata keçirilir. Fərqli stansiyalar eyni tezlikdə işləyə bilər, çünki modulyasiya zamanı müxtəlif psevdo-təsadüfi nümunələrdən istifadə edirlər. Telefon siqnalları həm göndərmə, həm də qəbul üçün eyni tezlikdən istifadə etməklə, lakin müxtəlif vaxt intervallarında Tezlik Bölmə Dupleksləmə (FDD) ilə interleaved olunur.

İstinad stansiyalarının gücü 20 Vt və ya daha az, terminalların gücü isə 250 mVt-dır. Eyni zamanda, istinad stansiyaları terminalların gücünü tənzimləyir, onu minimuma endirir, yüksək keyfiyyətli ötürməni təmin edir. Məlumat ötürmə sürətləri saniyədə 200 kbit/s ilə onlarla meqabit arasında dəyişir.

4G. 4G və ya dördüncü nəsil mobil şəbəkə standartı 3G və 2G standartlarının davamçısıdır. Bu standart BTİ tərəfindən IMT-Advanced (International Mobile Telecommunication Advanced) adı altında müəyyən edilmişdir və 4G üçün tələbləri ehtiva edir. 4G üçün məlumat ötürmə sürətinin yuxarı həddi artıq 100 Mbit/s-i (sürətli hərəkət edən obyektlər üçün) və yavaş hərəkət edən və ya stasionar olanlar üçün 1 Gbit/s-i keçir. 4G İP-ə əsaslanan geniş bant genişliyi ilə genişləndirilə bilən və təhlükəsiz mobil rabitə təklif edir, onun vasitəsilə nitqdən əlavə istifadəçiyə müxtəlif multimedia xidmətləri də ötürülə bilər. 4G WiMAX (40 Mbit/s) və LTE (Long Term Evolution, 100 Mbit/s) kimi texnologiyalara əsaslanır. Radio ötürülməsində istifadə olunan modulyasiya texnologiyası OFDMA-ya əsaslanır.

WLAN. WLAN və ya simsiz şəbəkə IEEE 802.11 seriyalı standartlarda müəyyən edilmişdir: IEEE802.11b, IEEE802.11g, IEEE 802.11n (cədvəl 6.1).

Cədvəl 6.1.

WLAN standartları

Standart	Tezlik (Ghz)	Buraxma qabiliyyəti (Mbps)	İcazə verilən kanalların sayı	Əhatə dairəsi (m)
IEEE802.11b	2.4	11	1	140 (38)
IEEE802.11g	2.4	54	1	140 (38)
IEEE 802.11n	2.4-5	600	4	250 (70)

Simsiz LAN (WLAN) simsiz lokal şəbəkələrdə radio rabitəsi üçün qaydalar və spesifikasiyaları müəyyən edən IEEE 802.11 seriyalı standartlarla müəyyən edilir. Bu standartlar müxtəlif cihazlar və şəbəkə komponentləri arasında uyğunluğu təmin edərək, eyni simsiz şəbəkədə birlikdə işləməyə imkan verir.

IEEE 802.11b standartı 1999-cu ildə təqdim edildi və simsiz şəbəkələr üçün ilk geniş yayılmış standartlardan biri oldu. O, 2,4 GHz tezliyində işləyir və maksimum 11 Mbit/s-ə qədər məlumat ötürmə sürətini dəstəkləyir. Bu standart HomeRF kimi əvvəlki texnologiyalar üzərində əhəmiyyətli təkmilləşdirmə təmin etdi və ev və ofis istifadəsi üçün məşhur oldu

2,4 GHz tezliyində də işləyən IEEE 802.11g standartı 2003-cü ildə hazırlanmışdır. O, 802.11b ilə müqayisədə daha yüksək ötürmə qabiliyyətini təmin edən 54 Mbps-ə qədər məlumat sürətini dəstəkləyir. 802.11g-nin mühüm üstünlüyü onun 802.11b kimi köhnə standartlara uyğunluğudur ki, bu da 802.11b ilə işləyən cihazlara 802.11g istifadə edən şəbəkələrlə qarşılıqlı işləməyə imkan verir.

2009-cu ildə yekunlaşdırılan IEEE 802.11n standartı əvvəlki versiyalarla müqayisədə əhəmiyyətli təkmilləşməni təmsil edir. O, iki tezlik diapazonunda işləyir: 2,4 GHz və 5 GHz. 802.11n ideal şəraitdə 600 Mbps-ə qədər maksimum məlumat ötürmə sürətinə imkan verən MIMO (Çoxlu Giriş Çoxlu Çıxış) texnologiyasından istifadə edərək çox axınlı məlumat ötürülməsini dəstəkləyir. Bu standart həmçinin əvvəlki versiyalarla müqayisədə təkmilləşdirilmiş etibarlılıq və əhatə dairəsi təmin edir.

Bu standartlar simsiz şəbəkələrin xüsusiyyətlərini, o cümlədən tezlik diapazonlarını, məlumat sürətlərini və müxtəlif cihazlar arasında uyğunluğu

təmin etmək üsullarını müəyyən edir. Onlar simsiz rabitə texnologiyalarının inkişafında əsas rol oynayır, sürətli və səmərəli simsiz şəbəkələrin yaradılmasına imkan verir.

Simsiz yerli şəbəkələrin (WLAN) istifadəsi onların üstünlüklərinin ənənəvi simli şəbəkələrdən çox olduğu bir sıra hallarda məqsədəuyğundur. WLAN çeviklik, rahatlıq və qənaəti təmin edir ki, bu da onu müxtəlif ssenarilər üçün uyğun edir. Əvvəlcə WLAN yüksək istifadəçi hərəkətliliyinin tələb olunduğu yerlərdə istifadə üçün idealdır. Bu, işçilərin tez-tez müxtəlif iş stansiyaları arasında hərəkət etdiyi və ya əməkdaşlıq sahələrində görüşdüyü ofislərdə xüsusilə doğrudur. Belə hallarda simsiz şəbəkələr müəyyən bir yerə bağlanmadan daimi əlaqə saxlamağa imkan verir. Bundan əlavə, WLAN çox sayda tələbə və müəllim üçün şəbəkə təmin etmək ehtiyacı olan məktəblər və universitetlər kimi təhsil müəssisələrində faydalıdır. Simsiz şəbəkə internetə və məktəb resurslarına çıxışı asanlaşdırır, istifadəçilərə kampusun istənilən yerindən şəbəkəyə qoşulmağa imkan verir. Yaşayış yerlərində WLAN kabel çəkməyə ehtiyac olmadan İnternetə və yerli resurslara rahat çıxışı təmin edir ki, bu da çoxmənzilli binalarda və ya yerin məhdud olduğu yerlərdə xüsusilə vacibdir. Simsiz şəbəkələr həmçinin smartfonlar, noutbuklar, planşetlər və ağıllı qurğular kimi müxtəlif cihazları kabel tıxacları yaratmadan birləşdirməyi asanlaşdırır.

Simsiz şəbəkələr həmçinin kafe, restoran və ticarət mərkəzləri kimi ictimai yerlərdə istifadə olunur, burada pulsuz Wi-Fi təmin etmək müştəri təcrübəsinin vacib hissəsidir. WLAN istifadəçilərə ziyarətçilərin təcrübəsini və məmnuniyyətini artıraraq İnternetə çıxışı təmin etməyə imkan verir. Bəzi hallarda, WLAN müvəqqəti şəbəkələr yaratmaq üçün istifadə olunur, məsələn, məhdud müddət ərzində iştirakçılara şəbəkəyə girişin təmin edilməli olduğu sərgilərdə, konfranslarda və ya tədbirlərdə. Simsiz şəbəkələr sizə kabel çəkməyə ehtiyac olmadan infrastrukturu tez yerləşdirməyə və konfiqurasiya etməyə imkan verir.

Nəhayət, simsiz şəbəkələr termostatlar, təhlükəsizlik kameraları və ağıllı işıq lampaları kimi bir çox cihazı birləşdirməyin çeviklik və konfiqurasiya asanlığını tələb etdiyi ağıllı evlərdə və Əşyaların İnternetində (IoT) istifadə olunur. WLAN bu cihazlar üçün etibarlı əlaqə təmin edərək, onları idarə etməyi və inteqrasiya etməyi asanlaşdırır. Beləliklə, WLAN çeviklik, hərəkətlilik və qoşulma asanlığı tələb edən müxtəlif vəziyyətlər üçün effektiv həll yolu təqdim edir.

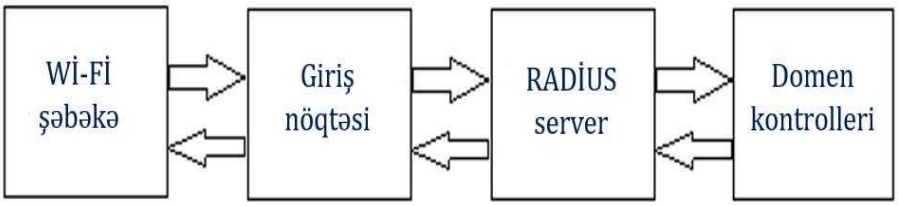
SİMSİZ TEXNOLOGİYANIN ƏSAS KOMPONENTLƏRİ VƏ PROTOKOLLARI

Simsiz yerli şəbəkə (WLAN) ilə sinonimi olan Wi-Fi texnologiyası iki əsas iş rejimini dəstəkləyir: infrastruktur və Ad-hoc.

İnfrastruktur rejimində şəbəkədəki qurğular mərkəzi mərkəz rolunu oynayan və simsiz müştərilərlə İnternet və ya daxili serverlər kimi digər şəbəkə resursları arasında əlaqə yaratmağa imkan verən giriş nöqtəsinə qoşulur. Giriş nöqtəsi bütün simsiz bağlantıları idarə edir, məlumatların yönləndirilməsini təmin edir və təhlükəsizliyin idarə edilməsi və şəbəkə performansının optimallaşdırılması kimi əlavə funksiyaları yerinə yetirə bilər. Bu rejim əksər ev və korporativ simsiz şəbəkələrdə istifadə olunur, çoxlu sayda istifadəçi və qurğular üçün sabit və mərkəzləşdirilmiş əlaqə təmin edir.

Ad-hoc rejimi, öz növbəsində, cihazlara mərkəzi giriş nöqtəsinə ehtiyac olmadan bir-biri ilə birbaşa əlaqə saxlamağa imkan verir. Bu rejimdə cihazlar hər bir cihazın bir qovşaq rolunu oynadığı və məlumatları birbaşa şəbəkədəki digər cihazlara ötürə biləcəyi müvəqqəti şəbəkə yaradır. Ad-hoc rejimi tez-tez giriş nöqtəsinin mümkün olmadığı və ya zəruri olmadığı hallarda, məsələn, yığıncaqda çoxsaylı noutbuklar və ya mobil cihazlar arasında faylları paylaşarkən müvəqqəti şəbəkələr yaratmaq üçün istifadə olunur.

Hər iki rejimin öz xüsusiyyətləri və tətbiq sahələri var. İnfrastruktur rejimi daha çox nəzarət və miqyaslılığı təmin edərək onu sabit şəbəkələr üçün üstünlük təşkil edir. Ad-Hock rejimi çeviklik və konfiqurasiya asanlığını təmin edərək onu qısamüddətli və qeyri-rəsmi şəbəkə əlaqələri üçün uyğun edir.Bu rejimdə siz simsiz şəbəkəyə istifadəçi girişini mərkəzləşdirilmiş şəkildə qoruya və idarə edə bilərsiniz. Korporativ şəbəkələrdə (müəssisə şəbəkələri) giriş nöqtələri adətən müxtəlif istifadəçilərin autentifikasiyası sorğularını əlaqələndirən və müəyyən edilmiş qaydalara uyğun olaraq şəbəkəyə girişə icazə verən və ya onu rədd edən RADIUS server (Remote and Dial-Up Service) vasitəsilə həyata keçirilir (şəkil 6.5).



Şəkil 6.5. RADIUS serverindən istifadə edərək WLAN şəbəkəsinin identifikasiyası

Simsiz əlaqə yaratmaq üçün ona qoşulan qurğuları bir-biri ilə uyğun olmalıdır. Bu məqsədlə müxtəlif cihazlar üçün standartlar hazırlanmışdır. Fərqli standartlara aid olan cihazlar eyni tezlikdə işləmələrinə baxmayaraq, çox vaxt uyğun gəlmir.

Simsiz internet tətbiq protokolu WAP-dır (Simsiz Tətbiq Protokolu). Simsiz Tətbiq Protokolu (WAP) köhnə mobil telefonlar və PDA-lar kimi resurs məhdud mobil cihazlar vasitəsilə İnternet proqramlarına və xidmətlərinə çıxışı təmin etmək üçün nəzərdə tutulmuş standartdır. 1990-cı illərin sonlarında hazırlanmış WAP məhdud hesablama gücü və kiçik ekranlı mobil qurğular üçün İnternet məzmunu və proqramları yerləşdirmək üçün yaradılmışdır. WAP aşağı bant genişliyi olan mobil şəbəkələr üzərində sürətli və səmərəli qarşılıqlı əlaqə yaratmaq üçün kompakt məlumat formatlarından və sadələşdirilmiş veb səhifələrdən istifadə edir. Protokolun əsas elementi mobil cihazların ekranlarında məlumatların göstərilməsi üçün xüsusi olaraq yaradılmış işarələmə dili olan Wireless Markup Language (WML)-dir. WML veb məzmunla naviqasiyanı və qarşılıqlı əlaqəni asanlaşdırır, onu mobil telefon istifadəçiləri üçün əlçatan və rahat edir. Protokol həmçinin müştəri cihazları və serverlər arasında etibarlı və səmərəli əlaqəni təmin edən əməliyyatları və məlumat ötürülməsini idarə edən Simsiz Transaction Protocol (WTP) daxildir. Simsiz Sessiya Protokolu (WSP) seans idarəçiliyini dəstəkləyir, müştəri ilə server arasında əlaqəni optimallaşdırır və etibarlı əlaqəni təmin edir. WAP HTTP və TCP/IP kimi mövcud İnternet protokolları ilə inteqrasiya etmək üçün nəzərdə tutulmuşdur və 2G və 3G daxil olmaqla müxtəlif növ mobil şəbəkələri dəstəkləyir. Bu, resursları məhdud olan cihazlarda istifadə üçün uyğunlaşdırılmış mobil veb proqramların və xidmətlərin yaradılmasına imkan verib.

WAP mobil internetin inkişafında mühüm addım olsa da, daha güclü mobil cihazların mövcudluğu və mobil rabitə texnologiyalarının təkmilləşməsi ilə zaman keçdikcə onun istifadəsi azaldı. Müasir mobil qurğular və veb-brauzerlər daha təkmil imkanlar, o cümlədən HTML5 dəstəyi və daha mürəkkəb veb proqramlar təklif edir ki, bu da WAP-ı daha az aktuallaşdırdı, lakin o, mobil texnologiyaların və veb proqramların inkişafında mühüm miras qoyub.

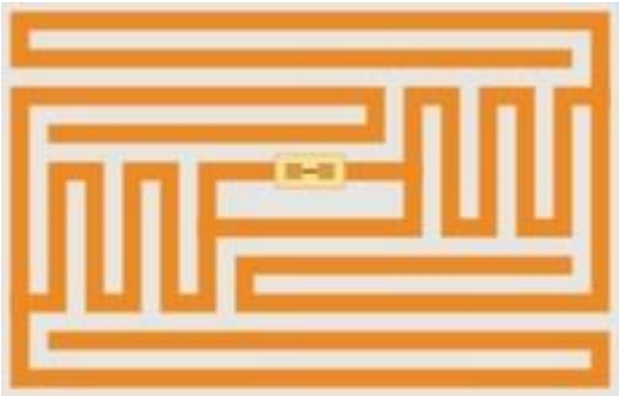
Mobil IP protokolu mobil cihazların müxtəlif şəbəkələr arasında hərəkət edərkən IP ünvanlarını saxlamağa imkan verən davamlı olaraq şəbəkəyə qoşulması üçün nəzərdə tutulmuşdur. Bu, noutbuklar, smartfonlar və planşetlər kimi yerləri tez-tez dəyişən cihazlar üçün xüsusilə vacibdir. Mobil İP, cihaz öz ev şəbəkəsindən kənarda olsa belə, şəbəkə ilə daimi əlaqə saxlamağa

imkan verməklə mobilliyə imkan verir. Bu, cari yerindən asılı olmayaraq, cihazın IP ünvanını dəyişməz saxlayan xüsusi mexanizmdən istifadə etməklə əldə edilir. Köçürülmə prosesi zamanı cihaz qoşulduğu şəbəkədən yeni müvəqqəti IP ünvanı alır, lakin onun ev IP ünvanı daimi olaraq qalır və cihazı müəyyən etmək və onunla əlaqə saxlamaq üçün istifadə olunur.

Mobil IP həm IPv4, həm də IPv6-da işləyir və müxtəlif IP protokol versiyaları ilə uyğunluq təmin edir. O, rabitə və marşrut məlumatlarını saxlamaq üçün birlikdə işləyən mobil qovşaqlar, ev agentləri və xarici agentlər kimi bir neçə əsas komponenti ehtiva edir. Mobil qovşaqlar şəbəkələr arasında hərəkət edən cihazlardır, ev agentləri cihazın cari yerinin qeydini idarə edir və xarici agentlər cihaz və şəbəkə arasında məlumatların ötürülməsinə kömək edir. Mobil İP-dən istifadə internet resurslarına və xidmətlərinə maneəsiz çıxış imkanı verir ki, bu da müxtəlif şəbəkələrə tez-tez qoşulmalarını dəyişən istifadəçilər üçün, məsələn, səyahət zamanı və ya ofislər və evlər arasında hərəkət edərkən xüsusilə vacibdir. Bu, aktiv əlaqələri saxlamağa və dəyişən şəbəkə mühitlərinə görə fasiləsiz işləməyə davam etməyə imkan verməklə istifadəçi təcrübəsini yaxşılaşdırır.

RFID (Radio Frequency Identification) RFID (Radio Frequency Identification) transponderlər və ya RFID teqləri adlanan xüsusi cihazlara məlumatları oxumaq və yazmaq üçün radiotezlik siqnallarından istifadə edən avtomatik obyekt identifikasiyası üsuludur. RFID sistemində etiketlər etiket və oxucu arasında radio əlaqəsi vasitəsilə ötürülə bilən məlumatları ehtiva edir.

RFID etiketi oxuyucunun əhatə dairəsinə daxil olduqda, oxucu etiketi aktivləşdirən və məlumatlarını geri ötürməyə imkan verən radio siqnalını işə salır. Teq növündən və sistemindən asılı olaraq, məlumat ya oxuna bilər, ya da etiketə yazıla bilər. RFID texnologiyası obyektlərin identifikasiyası və izlənilməsi prosesini avtomatlaşdırır, birbaşa əlaqə və ya vizual oxumağa ehtiyac olmadan sürətli və dəqiq məlumatların toplanmasını təmin edir. Bu texnologiya müxtəlif sahələrdə, o cümlədən inventarların idarə edilməsi, logistika, anbar proseslərinin avtomatlaşdırılması, giriş və nəzarət sistemlərində geniş istifadə olunur. RFID, ənənəvi identifikasiya üsulları ilə müqayisədə obyektlərin izlənilməsi və idarə olunması prosesini xeyli asanlaşdırır və sürətləndirir, səmərəliliyi artırır və səhvlərin baş vermə ehtimalını azaldır. (şəkil 6.6).



Şəkil 6.6. RFID etiketi

İstənilən RFID sistemi oxuma qurğusundan (oxuyucu, oxucu və ya sorğulayıcı) və transponderdən (həmçinin RFID etiketi kimi tanınır, bəzən RFID etiketi termini də istifadə olunur) ibarətdir. RFID-in işlədiyi mexanizmlər fərqli ola bilər, lakin adətən rabitə RFID etiketinin dizaynına uyğun olaraq cavab verməli olduğu bir siqnal ilə elektromaqnit dalğaları göndərən bir oxucu ilə başlayır. RFID etiketi oxuyucu siqnalını modullaşdırır və ondan rəqəmsal məlumatları çıxaran oxucuya geri göndərir. Real vaxt rejimində yerləşdirmə sistemləri oxucu siqnallarına reaksiya vermir, müəyyən fasilələrlə öz təşəbbüsü ilə siqnallar göndərir. Oxucu siqnalı qəbul edir və onun proqramı RFID etiketinin yerini hesablayır.

KRİPTOQRAFİYA VƏ ŞİFRƏLƏMƏ PROTOKOLLARI

Kriptoqrafiya informasiyanın gizlədilməsi sənəti olmaqla yanaşı, həm də məlumatın məxfiliyini (məlumatın kənar şəxslər tərəfindən oxunmasının mümkünsüzlüyü) və həqiqiliyini (müəllifliyin bütövlüyü və həqiqiliyi, habelə müəlliflikdən imtinanın mümkünsüzlüyü) təmin etmək üsulları haqqında elmdir. Məlumatın göndəricisi verilənləri bəzi alqoritmlərlə göndərməzdən əvvəl emal edir (məlumatları şifrələyir), məlumatı qəbul edən şəxs məlumatı anlamaq üçün uyğun formada deşifrə yəni əks əməliyyat həyata keçirir. Ənənəvi şifrələmə mexanizmi ondan ibarətdir ki, verilənlərə açara əsaslanan bir növ şifrələmə metodu tətbiq edilir, bundan sonra verilənlər oxunmaz hala gəlir. Onu ancaq açarı bilən adam oxuya bilər. Açarın uzunluğu şifrələmənin

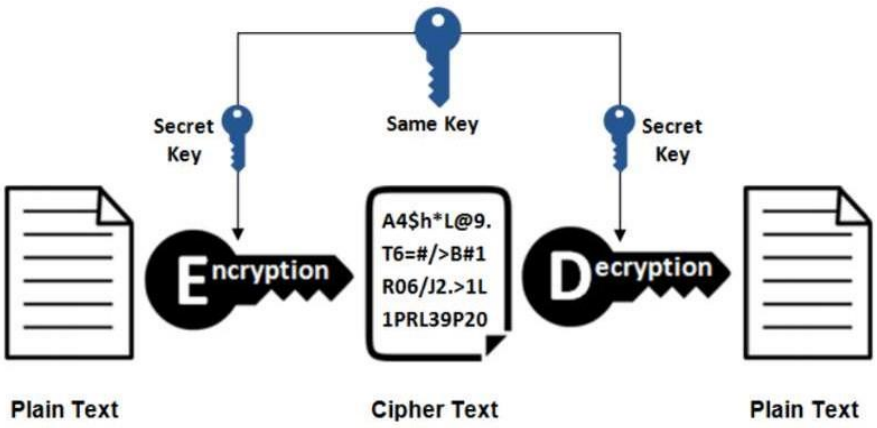
mürəkkəbliyini müəyyən edir. Açar nə qədər uzun olsa, “kobud” qüvvə ilə sındırmaq bir o qədər çətindir. Müasir yüksək təhlükəsizlik alqoritmləri uzunluğu 256 bit (məsələn, AES) və ya 512-4096 bit (məsələn, RSA) olan açarlardan istifadə edir. Bəzi alqoritmlər açarı dinamik şəkildə dəyişmək üçün daxili imkanlara malikdir. Bu o deməkdir ki, eyni açar məhdud zaman ərzində etibarlıdır. Yeni alqoritmlərin işlənib hazırlanmasında ixtisaslaşan mütəxəssislərə kriptoqraflar, kodların pozulmasında ixtisaslaşanlara isə kriptoanalitiklər deyilir. Məlumdur ki, kriptoqrafiyanın tarixi 4000 il əvvələ gedib çıxır. İlk kriptosistemlər eramızdan əvvəl V əsrdə Spartada işlənmiş "Spartalı Scytale" metodu adlandırılmışdır. Şifrələnmiş mətn çubuq uzunluğunda perqament zolağına yazılır, çubuq bitdikdən sonra çevrilir və növbəti mətn yazılmağa başlayır. Deşifrə eyni diametrli bir çubuqdan istifadə etməklə həyata keçirilirdi.

İlk kripto koduna mesajdakı hərflərin verilmiş yerdəyişmə ilə əlifbada olan digərləri ilə əvəz edildiyi "Sezar kodu" daxildir, əgər siz xüsusi hərflərin görünüşünün tezliyi təhlilindən istifadə edirsinizsə, bu cür kodların sınması nisbətən sadədir mətn nəzərə alır ki, hər bir dildə ayrı-ayrı hərflərin görünüşü öz (məlum) tezliyinə malikdir. Şifrələmə alqoritmlərini iki növə bölmək olar:

Simmetrik açar alqoritmləri.

Asimmetrik açarı olan alqoritmlər.

Simmetrik açar şifrələməsi halında, şifrələmə və şifrənin açılması hər iki tərəfə məlum olan eyni açarla həyata keçirilir (şəkil 6.7).



Şəkil 6.7. Simmetrik açar şifrələmə mexanizmi

Bu alqoritm vəziyyətində şifrələmə açarını gizli saxlamaq vacibdir. Açar üçüncü tərəfə məlum olarsa, məlumat artıq qorunmur. Bu açarı şəbəkə üzərindən təhlükəsiz şəkildə ötürmək mümkün deyil, lakin onu ötürmək üçün alternativ üsullardan istifadə edilməlidir (adi poçt və ya poçt daşıyıcısı vasitəsilə göndərmə). Bu problemlidir və təhlükəsizliyə zəmanət vermir.

Simmetrik açar şifrələməsinin dezavantajı ondan ibarətdir ki, o, açarın informasiyaya baxa bilən hər kəsə paylanmasını tələb edir. Amma məlumdur ki, açar onlarla insana məlumdursa, o zaman informasiyanın gizli qalması çətin prosesdir. Bəzi şifrələmə üsulları əvvəlcə müəyyən miqdarda məlumatın şifrələndiyi və sonra növbəti bloku şifrələməyə davam etdiyi bir blok şifrəsindən istifadə edir, digərləri isə şifrələmənin bit-bit baş verdiyi axın şifrəsindən istifadə edir (və ya bayt bayt). Simmetrik alqoritmlər geniş istifadə olunur və kifayət qədər mürəkkəblik nəzərə alınmaqla, onları pozmaq asan deyil. Ən geniş yayılmış simmetrik şifrələmə alqoritmlərinə aşağıdakılar aiddir:

Data şifrələmə standartı (DES) uzun müddətdir istifadə olunur və rəsmi qurumlar tərəfindən tanınan ilk standartdır. Bu günə qədər AES alqoritmləri ilə əvəz edilmişdir. DES 56 bitlik açar uzunluğundan istifadə edir. Hazırda onu sındırmaq bir neçə günün işidir.

Triple-DES (3DES) DES alqoritminin daha təhlükəsiz versiyasıdır.

Təkmilləşdirilmiş şifrələmə standartı (AES) Rijndael alqoritmlərindən istifadə edir. AES indi ABŞ dövlət qurumları tərəfindən istifadə edilən əsas şifrələmə yanaşmasıdır. Bu standart 256 bitə qədər açar şifrələməsini dəstəkləyir.

Rivest's Cipher (RC) RSA laboratoriyaları tərəfindən hazırlanmış bir alqoritmdir. Müasir versiyalar RC5 və RC6-dır. RC5 2048 bitlik açardan istifadə edir.

Simmetrik şifrələmənin üstün cəhətlərinə daxildir:

- Şifrələmə və deşifrə üçün tək açardan istifadə etdiyi üçün onu icra etmək daha sürətli olur.

- Alıcının şəxsiyyətini sübut etmək üçün təhlükəsizlik məqsədi kimi parol identifikasiyasından istifadə edir.

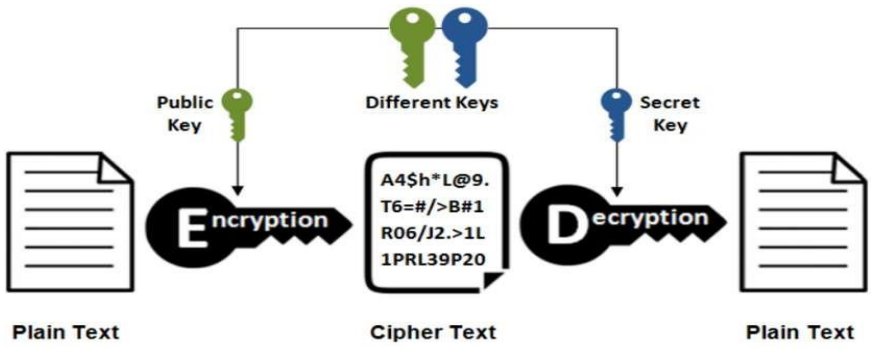
- İstifadəçilərin şifrələmə və deşifrə üçün yalnız bir açarı var ki, onu icra etmək və idarə etmək asandır.

Simmetrik şifrələmənin mənfi cəhətlərinə daxildir:

- Şifrələmə açarlarını təhlükəsiz şəkildə paylaşmaq şansları daha azdır; Simmetrik Şifrələmədə açarları bölüşmək çətin və çətindir.

-Simmetrik o qədər də genişləndirilə bilməz, çünki müxtəlif istifadəçilər üçün uyğun deyil.

Asimmetrik şifrələmə protokolu bir cüt açardan istifadə edir - ictimai və özəl. Açıq açar məlumatı şifrələmək üçün, şəxsi açar isə onun şifrəsini açmaq üçün istifadə olunur (şəkil 6.8.). Asimmetrik şifrələmə alqoritmləri sındırıla bilməyən bir cüt təşkil edən iki açardan istifadə edir. Açarların yaradıcısı özü üçün bir açar saxlayır: bu açar şəxsi (özəl) adlanır. İkinci açar dərc olunur. Buna açıq (ictimai) açar deyilir.



Şəkil 6.8. Asimmetrik şifrələmə

Asimmetrik şifrələmə vəziyyətində məlumat mübadiləsinin hər bir subyektinin bir cüt şəxsi və açıq açarları olmalıdır. Təhlükəsizlik alqoritmin mürəkkəbliyi ilə təmin edilir ki, bu da birinci komponenti bilməklə açar cütünün ikinci komponentini əldə etmək imkanını aradan qaldırır.

Asimmetrik şifrələmə resurs və vaxt aparan olduğundan, praktikada verilənləri şifrələmək üçün adətən simmetrik alqoritmdən istifadə edilir və açarlar məlumat alıcının açarı ilə asimmetrik şifrələmə alqoritmi ilə paylanır. Məsələn, e-poçt elə şifrələnir ki, mesajın məzmunu xüsusi yaradılmış (simmetrik) açarla, açar isə öz növbəsində mesajı qəbul edənin açıq açarı ilə şifrələnir. Şifrələnmiş açar alıcıya göndərilir, o, şəxsi açarından istifadə edərək onu deşifrə edə bilər.

Hazırda aşağıdakı asimmetrik şifrələmə alqoritmlərindən istifadə olunur:

RSA alqoritminin adı onun yaradıcılarının adlarının baş hərfindən formalaşmışdır: Ron Rivest, Adi Şamir və Leonard Adleman. RSA şifrələmə üçün böyük əsas nömrələrdən istifadə edir və təkmilləşdirilmiş açıq açar infrastrukturlarından (PKI - Açıq Açar İnfrastruktur) istifadə edir. RSA alqoritmləri həm şifrələmə, həm də rəqəmsal (elektron) imza yaratmaq üçün

geniş tətbiq olunur. RSA müxtəlif mühitlərdə, o cümlədən SSL (Secure Sockets Layer) texnologiyasından istifadə edərək təhlükəsiz rabitə kanalının yaradılması zamanı istifadə olunur. Simmetrik açarın heç bir yerə ötürülmədiyini qeyd etmək vacibdir, çünki o, tərəfdaşların hər biri üçün birbaşa "yerində" yaradılır.

Diffie-Hellmann açar mübadiləsi onun yaradıcılarının adını daşıyır. Onların ictimai-özəl açar cütü metodologiyasının əsasını qoyduğu güman edilir. O, ilk növbədə qlobal şəbəkələrdə açarları təhlükəsiz şəkildə göndərmək üçün istifadə olunur.

Elliptik əyri kriptosistem (ECC - Elliptic Curve Cryptography) öz işinə görə RSA alqoritminə bənzəyir. Əsasən kiçik sistemlərdə (mobil telefonlar və simsiz cihazlar kimi) istifadə olunur. ECC daha yığcamdır və daha az hesablama resursları tələb edir.

Asimmetrik şifrələmənin üstün cəhətlərinə daxildir:

- Asimmetrik Şifrələmə iki açara malikdir, biri açıq və biri özəldir, ona görə də açarların paylanması ilə bağlı heç bir problem yoxdur.

- Yenə də, bir cüt açarla birdən çox tərəflə ünsiyyət qurmaq çətin deyil və bu, böyük şəbəkələrdə daha genişlənə bilir.

Asimmetrik şifrələmənin mənfi cəhətlərinə daxildir:

- Asimmetrik Şifrələmə Simmetrik Şifrələmə ilə müqayisədə performans baxımından daha yavaşdır.

- Asimmetrik Şifrələmə böyük açar ölçülərinə görə həyata keçirmək və idarə etmək o qədər də asan deyil.

Məlumatların ötürülməsində kriptoqrafiyanın istifadəsi məlumatların məxfiliyini, bütövlüyünü və həqiqiliyini təmin etməyə kömək edir.

Məxfilik sistemi icazəsiz girişdən qorumaqdır. Kritik alqoritm bunun qarşısını almaq üçün kifayət qədər güclü olmalıdır. Alqoritmin gücü, alqoritmləri pozmaq üçün tələb olunan vaxt və cəhdin qiymətləndirilməsi kimi iş amili ilə xarakterizə olunur.

Dürüstlük, məlumatın ünvana çatdığı zaman etibarlılıq və tamlıq tələbidir (onun həm müdaxilələrdən, həm də şəbəkə problemlərindən qorunması). Bunun üçün onun şifrəsini açarkən istifadə edilə bilən yoxlama sayı və ya məlumatların təkrarlanması üsulu istifadə olunur. Dürüstlük maraqları naminə, göndərənin həqiqiliyini təmin edən rəqəmsal imza texnologiyasından da istifadə edilə bilər.

Elektron rəqəmsal (rəqəmsal) imza adi imzada olduğu kimi imza sahibini müəyyən etməyə imkan verir. Göndərilən zaman, şifrələnmiş mesaja şəxsi açar

əlavə olunur ki, bu da mesajın alıcısına onun yaradıcısını unikal şəkildə müəyyən etməyə imkan verir. Avtorizasiya zamanı göndərənin özünün iddia etdiyi şəxs olması nəzarət edilir. Avtorizasiya üçün ümumi yanaşma rəqəmsal imza texnologiyasından istifadə etməkdir. Avtorizasiya əvvəlcədən razılaşdırılmış paroldan istifadə etməklə də idarə oluna bilər.

İnkar etməmək, açıq açarın istifadəçisinin özünün iddia etdiyi şəxs olduğuna inamı qorumaq mexanizmidir. Bunun üçün onlar imza açarı sertifikatından - sertifikatlaşdırma orqanının səlahiyyətli şəxsinin (CA - Sertifikatlaşdırma orqanı) rəqəmsal imzası olan elektron sənəddən istifadə edirlər, o, öz açarları ilə eyniləşdirmə və avtorizasiya sertifikatlarını verir və saxlayır.

Açıq açar arxitekturası (PKI - Public Key Infrastructure) məlumatların təhlükəsiz ötürülməsi ilə əlaqəli müxtəlif təhlükəsizlik aspektlərini birləşdirir. PKI – məlumatların təhlükəsiz ötürülməsini təmin etmək və ticarət sirlərini qorumaq üçün e-biznesdə istifadə olunur. PKI aşağıdakı komponentləri ehtiva edən asimmetrik şifrələmə sistemidir:

Sertifikat orqanı sertifikatları verir, ləğv edir və saxlayır. Mərkəz ictimai (hamılıqla tanınan üçüncü tərəf) və ya özəl (sertifikasiya daxili həyata keçirilir) ola bilər.

Açıq və şəxsi açarları yaratmaq üçün şifrələmə alqoritmi (məsələn, RSA).

Rəqəmsal sertifikatlar açarı müəyyən bir şəxsiyyət ilə asinxron şəkildə birləşdirən mexanizmlərdir. PKI sistemindəki hər bir istifadəçinin ona icazə verməк üçün istifadə edilə bilən sertifikatı var. Ən çox yayılmış sertifikatlaşdırma standartı X.509-dur. Bu standart sertifikatda olan məlumatları (versiya, seriya nömrəsi, alqoritm, verən orqan, etibarlılıq müddəti, sertifikatın alıcısı, istifadə məqsədi, açarlar və s.) müəyyən edir. Mövcud olmalı və sertifikatın etibarlılığının yoxlanıla biləcəyi siyahı (CRL - Sertifikatın ləğvi siyahısı) var.

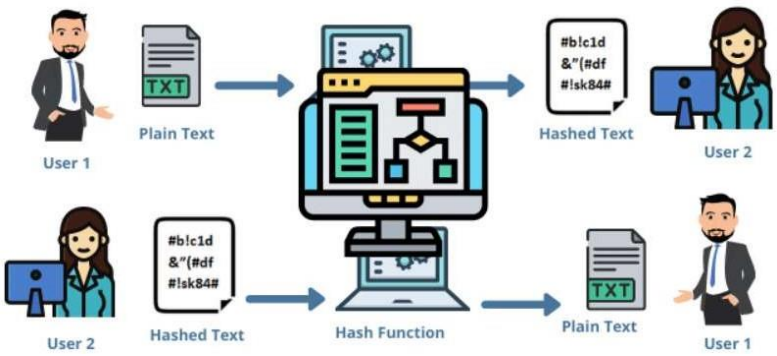
Xeşləmə (Hashing), ixtiyari miqdarda daxil edilmiş məlumatdan sabit bir məlumat ölçüsünü (heş dəyəri və ya hash kodu adlanır) yaratmaq üçün istifadə olunan kriptoqrafik bir texnikadır. Bu proses məlumatların göndərilmədən əvvəl gizlədilməsi deyil, bütövlüyünü təmin etmək məqsədi ilə yanaşı gedir (şəkil 6.9). Hashing prosesində daxil edilən məlumatlar hash funksiyası ilə işlənir və onu unikal sabit təmsilə (hesh dəyəri) çevirir. Hash funksiyaları aşağıdakı xüsusiyyətlərə malikdir:

- Eyni giriş məlumatlarını nəzərə alaraq, eyni hash funksiyası həmişə eyni hash dəyərini yaradacaq.

- Haş dəyərinin ölçüsü sabitdir, yəni giriş məlumatının ölçüsündən asılı olmayaraq, hash dəyəri həmişə eyni uzunluqda olacaqdır.

- Haş funksiyaları adətən birtərəfli olur, yəni hash dəyərindən orijinal məlumatları yenidən qurmaq çox çətindir (faktiki olaraq qeyri-mümkündür).

- İdeal haş funksiyası toqquşmaların qarşısını almaq üçün müxtəlif girişlər arasında hash dəyərlərinin bərabər paylanmasını təmin etməlidir (müxtəlif girişlərin eyni hash dəyərinə malik olduğu vəziyyətlər).



Şəkil 6.9. Xeş protokolu

Hashing verilənlər bazası parolları, fayl yoxlama məbləğləri, rəqəmsal imzalar və digər kriptoqrafik və informasiya təhlükəsizliyi proqramları kimi məlumatların bütövlüyünü yoxlamaq üçün geniş istifadə olunur. Bununla belə, yadda saxlamaq lazımdır ki, hashing məlumatı gizlətmək məqsədi daşımır; hash dəyərləri orijinal məlumatdan asanlıqla hesablana bilər, lakin əks proses (hesh dəyərindən orijinal məlumatın bərpası) adətən toqquşma hücumları və ya digər kriptoqrafik hücumlardan istifadə etmədən mümkün deyil.

Mühafizə protokolları. SSL (Secure Sockets Layer) protokolu TCP əsasında kompüterlər arasında təhlükəsiz rabitə kanalı yaratmaq üçün istifadə olunur. Protokolun yaradıcısı Netscape-dir. SSL rabitə seansı yaradarkən və açarları ötürərkən asimmetrik şifrələmədən istifadə edir, lakin verilənlərin ötürülməsi zamanı simmetrik şifrələmədən istifadə olunur. Bu protokol əlaqə seansı yaratmaq üçün dialoq (əl sıxma) metodundan istifadə edir (sessiya səviyyəsində). Eyni zamanda, tərəflər kiminlə məşğul olduqlarına və tərəfdaşın kommunikasiya xəttində dəyişdirilməməsinə inam qazanırlar. Dialoq əsasında tərəflər məlumatların sürətli ötürülməsi üçün ümumi simmetrik açar

hazırlayırlar. Əgər dialoq zamanı avtorizasiya ilə bağlı problemlər yaranarsa

(sertifikatlarla), o zaman müvafiq veb proqram bu barədə məlumat verir və təhlükə barədə xəbərdarlıq edir. Avtorizasiya uğurlu olarsa, müştəri simmetrik açar yaratmaq üçün məlumatları hazırlayır və serverin açıq açarından istifadə edərək göndərir. Müştərinin icazəsi tələb olunarsa, sonuncu imzalanmış sertifikatlarını göndərir. Server simmetrik açar yaratmaq üçün istifadə olunan yekun məlumat paketini hazırlayır. SSL dialoqunun addımları burada ətraflı təsvir edilmişdir:

http://support.microsoft.com/kb/q257591/

Nəqliyyat səviyyəsinin təhlükəsizliyi protokolu (TLS - Nəqliyyat səviyyəsinin təhlükəsizliyi) SSL protokolundan yaranan və gələcəkdə onu əvəz edə bilən bir protokoldur.

Secure Shell protokolu (SSH) əlaqə yaratmaq və avtorizasiyanı həyata keçirmək üçün açıq açardan istifadə edir. Kompüterə təhlükəsiz uzaqdan daxil olmaq üçün, həmçinin SFTP (Secure File Transfer Protocol) protokolundan istifadə edərək məlumatların ötürülməsi üçün istifadə olunur.

İnternet – verilənlərin mühafizəsi protokolu (IPSec - IP Təhlükəsizliyi) şifrələmə ilə şəbəkə üzərindən məlumatların hərəkətini təmin etmək üçün protokollar toplusudur. İnternet üzərindən ikitərəfli identifikasiya və şifrələmə imkanı verir. Protokolların iki əsas komponenti IP başlığıdır (AH - Authentication Header), onun köməyi ilə məlumat paketləri rəqəmsal imzalana bilər (ESP - Encapsulated Security Payload) və məlumat paketləri AES və ya 3DES alqoritmləri ilə şifrələnə bilər.

Virtual şəxsi şəbəkə (VPN - Virtual Şəxsi Şəbəkə) şifrələnmiş kanal vasitəsilə məlumatları bir kompüterdən digərinə göndərməyə imkan verir. Nöqtədən Nöqtəyə Protokolundan (PPP) istifadə edərək müştəri ilə server arasında şifrələnmiş kanal qurulur. PPP əlaqələri yaradıldıqda, onlar məlumatı şəbəkə üzərindən hərəkət marşrutu haqqında məlumatı ehtiva edən başlıq ilə təmin edirlər. VPN bağlantısı qlobal şəbəkədən (İnternet) yerli şəbəkəyə təhlükəsiz giriş əldə etmək üçün standart həlldən istifadə edir. Müxtəlif protokollardan istifadə olunur:

PPTP (Point to Point Tunneling Protocol) protokolu uzun müddətdir istifadə olunur və müxtəlif sistemlərlə yaxşı uyğunlaşır. Sertifikat icazəsi tələb etmir. Əlaqə yaradarkən dialoq (əl sıxma) şifrələnməmiş formada həyata keçirilir ki, bu da PPTP protokolunun ən böyük zəifliyidir. Protokol istifadəçi avtorizasiyası üçün PPP və 40-bit, 56-bit və ya 128-bit açarla MPPE (Microsoft Point to Point Encryption) məlumat şifrələməsindən istifadə edir.

L2TP (Layer 2 Tunneling Protocol) PPP icazəsi və IPsec şifrələməsindən istifadə edir və sertifikatlarla müştəri kompüterinin icazəsini tələb edir. PPP paketləri məlumatı WAN üzərindən nəql etmək üçün L2TP istifadə edərək kapsullaşdırılır. IPsec ESP L2TP trafikini şifrələyir. 256 bitə qədər AES şifrələməsi dəstəklənir.

SSTP (Secure Socket Tunneling Protocol) SSL protokolu üzərində PPP istifadə edir. SSTP standart olaraq müştəri autentifikasiyasını tələb etmir, lakin server əlaqə qurmazdan əvvəl müştərinin yoxladığı sertifikatları təqdim etməlidir.

IPv4 və ya IPv6	TCP	SSTP	PPP	IPv4 və ya IPv6
		SSL seansının mühafizəsi		

IKEv2 (Internet Key Exchange V2) avtorizasiya üçün IPSec şifrələməsindən istifadə edir, server öz şəxsiyyətini sertifikatla təsdiq etməlidir; Avtomatik əlaqə bərpasını dəstəkləyir (VPN Reconnect).

Beləliklə, şifrələmə protokolları[32] internet kimi təhlükəsiz şəbəkələr üzərindən keçərkən məlumatların məxfiliyini, bütövlüyünü və həqiqiliyini qorumaq üçün istifadə olunan qaydalar və prosedurlar toplusudur. Onlar icazəsiz girişdən, həmçinin ötürülmə zamanı məlumatların dəyişdirilməsindən və ya dəyişdirilməsindən qorunma təmin edir. Şifrələmə protokollarının məqsədi qorunmayan şəbəkələr üzərindən ötürülən məlumatların məxfiliyini, bütövlüyünü və həqiqiliyini təmin etməkdir. Onlar əməliyyatlar, həssas məlumatlar və mesajlaşma da daxil olmaqla onlayn təhlükəsizlikdə əsas rol oynayırlar. Şifrələmə protokollarından istifadə edilmədən məlumatlar təcavüzkarlar tərəfindən təhlükəyə məruz qala bilər ki, bu da məlumat sızmasına və ya digər ciddi təhlükəsizlik nəticələrinə səbəb ola bilər.

---

32 http://www.pcworld.com/article/2858642/you-can-encrypt-your-hard-drive-but-the-protection-may-not-be-worth-the-hassle.html
https://answers.syr.edu/display/software/Encrypting+your+external+hard+drive+on+Windows+and+OSX
http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946
http://blogs.microsoft.com/cybertrust/2012/07/31/microsofts-free-security-tools-series-introduction/
https://blogs.microsoft.com/cybertrust/2013/01/15/microsoft-free-security-tools-microsoft-security-compliance-manager-tool-scm/
Олифер В.Г. Безопасность компьютерных сетей. М.: Горячая линия - Телеком, 2018. 644с.
Олифер В.Г., Новые технологии и оборудование IP-сетей / В.Г.Олифер, Н.А.Олифер. – СПб.; БХВ-Петербург, 2021. 1005 с.

MAC ÜNVAN FİLTRLƏMƏ

MAC ünvan filtrasiyası[33] marşrutlaşdırıcılar və ya açarlar kimi şəbəkə avadanlığının MAC ünvanlarına əsasən hansı cihazların şəbəkəyə qoşula biləcəyi barədə qərar qəbul etdiyi şəbəkəyə girişə nəzarət üsuludur. MAC ünvanı (Media Access Control ünvanı) yerli şəbəkədə onları müəyyən etmək üçün şəbəkə interfeyslərinə (adətən şəbəkə kartları) təyin edilmiş unikal identifikatordur. MAC ünvanlarının filtrlənməsinin arxasında duran ideya ondan ibarətdir ki, şəbəkə avadanlığı MAC ünvanlarına əsasən cihazlara şəbəkə girişinə icazə vermək və ya bloklamaq üçün konfiqurasiya edilə bilər. Bu, şəbəkə administratorlarına şəbəkəyə girişi idarə etməyə imkan verir, onu yalnız icazəsi olan cihazlarla məhdudlaşdırır.

MAC ünvanlarının filtrlənməsinin məqsədi əlavə təhlükəsizlik səviyyəsini və şəbəkəyə giriş üzərində nəzarəti təmin etməkdir. MAC ünvan filtrləməsinin tətbiq olunduğu sahələrə daxildir:

- Şəbəkə administratorları MAC ünvanının filtrasiyasını yalnız İcazə Verilən Ünvanlar siyahısında əvvəlcədən qeydiyyatdan keçmiş xüsusi cihazlara və ya cihaz qruplarına girişə icazə vermək üçün konfiqurasiya edə bilərlər.

- MAC ünvanının filtrasiyası icazəsiz cihazların və ya təcavüzkarların şəbəkənizə qoşulmasının və şəbəkəyə daxil olmaq cəhdinin qarşısını alır.

- MAC ünvan filtrindən xüsusi cihazlar üçün prioritet girişi təmin etməklə İnternet və ya daxili şəbəkə xidmətləri kimi şəbəkə resurslarına girişi idarə etmək üçün istifadə edilə bilər.

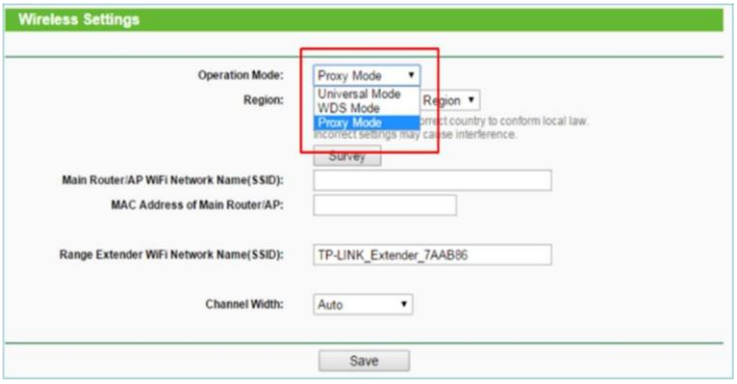
MAC ünvan filtri şəbəkəyə giriş nəzarətinin əlavə qatını təmin etsə də, MAC ünvanının xüsusi proqram təminatı vasitəsilə saxtalaşdırıla və ya dəyişdirilə biləcəyini xatırlamaq vacibdir. Buna görə də, şəbəkənizi daha da qorumaq üçün Wi-Fi üçün WPA2/WPA3 və ya şəbəkə sertifikatları kimi əlavə identifikasiya və təhlükəsizlik üsullarından istifadə etmək tövsiyə olunur.

MAC ünvan filtrləmə texnikasını nümunə göstərmək üçün MAC ünvanlarının filtrasiyası birbaşa marşrutlaşdırıcıya deyil, diapazon genişləndiricisinə qoşulmuş müştəriləri idarə etməyə yönəldilmişdir.

33

https://www.howtonetwork.com/comptia-network-study-guide-free/
https://moodle.kstu.ru/mod/page/view.php?id=9364
https://www.coursera.org/courses?query=information%20security

A hissəsi. Əvvəlcə siqnal genişləndiricinizin marşrutlaşdırıcıya uğurla qoşulduğundan əmin olun və siqnal genişləndiricinizin hansı rejimdə işlədiyini yoxlayın. Default olaraq Proxy rejimi seçilir (şəkil 6.10).



Şəkil 6.10. Rejimin təyini

Fərz edək ki, şəbəkə topologiyası şəkil 6.11-da təsvir olunmuşdur.

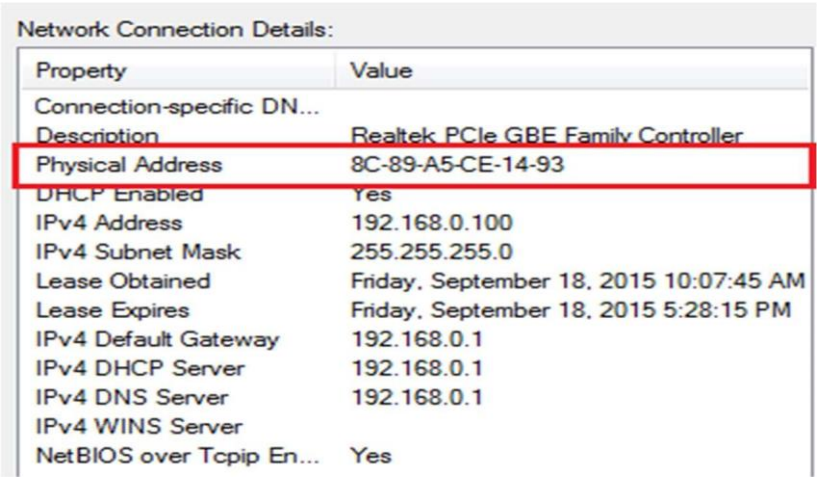
Şəkil 6.11. Şəbəkə topologiyası

Siqnal gücləndirici Proksi rejimindədirsə aşağıdakı xüsusiyyətlər təyin olunur.

1. Proksi rejiminin xüsusiyyətləri.

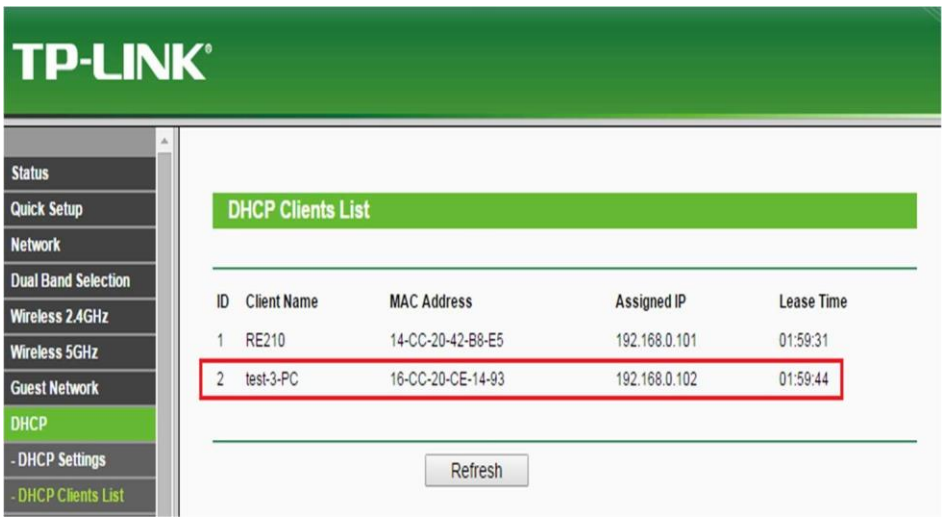
Proksi rejimində siqnal genişləndiricisi müştərinin hər bir real MAC ünvanını avtomatik olaraq yaratdığı virtual MAC ünvanı ilə əvəz edir. Beləliklə, marşrutlaşdırıcı müştərinin virtual MAC ünvanını real MAC ünvanı kimi qəbul edəcək, ona görə də biz bu müştərilərin virtual MAC ünvanlarını onların real MAC ünvanları əvəzinə marşrutlaşdırıcıda MAC ünvanlarının filtrasiya cədvəlinə daxil etməliyik. Aşağıdakı variantları müqayisə edərək, prosesi daha yaxşı başa düşə bilərsiniz.

a. Aşağıdakı şəkildə göstərildiyi kimi kompüterinizin MAC ünvanını yoxlayın. Kompüterinizin əsl MAC ünvanı 8C-89-A5-CE-14-93-dür (şəkil 6.12).



Şəkil 6.12. MAC ünvan

b. Sonra, marşrutlaşdırıcının veb səhifəsində göstərilən kompüterinizin MAC ünvanını yoxlayın. Kompüterinizin virtual MAC ünvanı 16-CC-20-CE-14-93-dür (şəkil 6.13).



Şəkil 6.13. Virtual MAC ünvanı

İndi görürsünüz ki, marşrutlaşdırıcı yalnız kompüterinizin virtual MAC ünvanını göstərir, onun real MAC ünvanını deyil. Xəbərdar olmaq üçün vacib bir

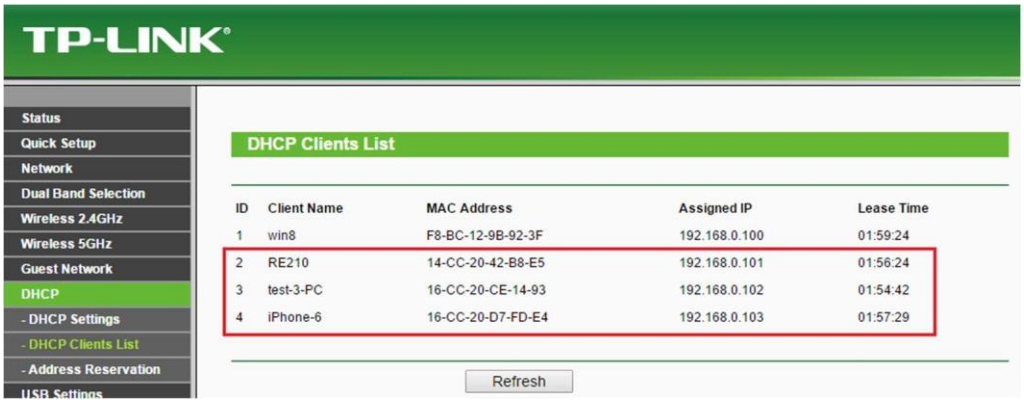
detal var, hər bir müştərinin virtual MAC ünvanının son 24 biti müştərinin real MAC ünvanının son 24 biti ilə tam olaraq eynidir.

Yuxarıdakı kompüterin real MAC ünvanını (8C-89-A5-CE-14-93) virtual MAC ünvanı ilə (16-CC-20-CE-14-93) müqayisə edərək qaydanı asanlıqla tapa bilərsiniz.

2. Gücləndiriciyə qoşulmuş müştərilərin virtual MAC ünvanlarını təyini.

a. Müştəri cihazlarınızın həqiqi MAC ünvanını yoxlayın və onları yazın. Bu müştəri cihazlarının virtual MAC ünvanlarına ehtiyacınız olacaq.

b. Routerinizin veb interfeysinə daxil olun və DHCP müştəri siyahısına keçin. Burada marşrutlaşdırıcı tərəfindən verilən cihazların bütün MAC ünvanlarını və IP ünvanlarını görürük. Bu MAC ünvanlarının son 24 bitini müştəri cihazlarınızın ünvanlarının son 24 biti ilə müqayisə edərək, müştəri cihazlarınızın virtual MAC ünvanlarını asanlıqla tapa bilərsiniz. Onları yazın. Onlara sonra ehtiyacınız olacaq (şəkil 6.14.).



Şəkil 6.14. Virtual MAC ünvanın xüsusiyyətlər pəncərəsi

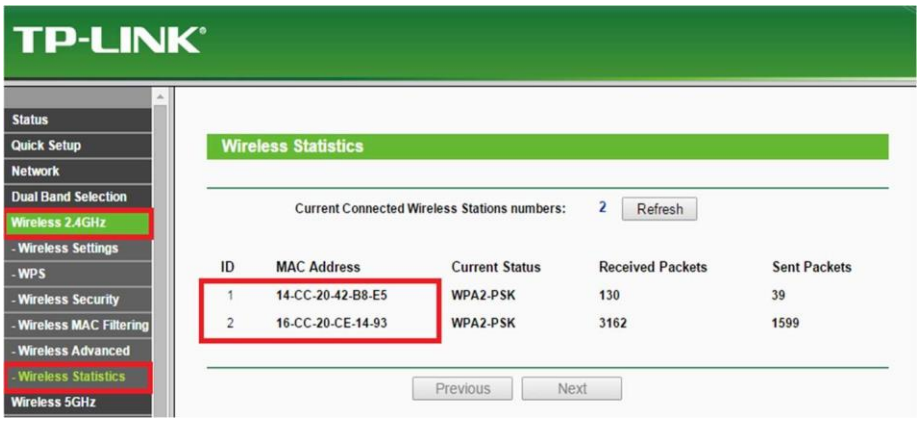
Qeyd: Routerinizin DHCP müştəri siyahısını necə yoxlamaq lazım olduğunu bilmirsinizsə, kömək üçün marşrutlaşdırıcı istehsalçınızla əlaqə saxlayın.

3. Siqnal genişləndiricisinin MAC ünvanlarının təyini.

TL-WA850RE kimi tək diapazonlu siqnal genişləndiricisinin 2,4 GHz-də bir MAC ünvanı, ikili diapazonlu siqnal genişləndiricisinin isə müvafiq olaraq 2,4 GHz və 5 GHz-də istifadə olunan iki MAC ünvanı var.

a. Routerinizin veb interfeysinə daxil olun və Simsiz 2.4GHz -> Simsiz Statistikanı seçin, 2.4GHz-də marşrutlaşdırıya qoşulmuş cihazların MAC ünvanlarını görəcəksiniz. Bu MAC ünvanlarını siqnal gücləndiricinizin

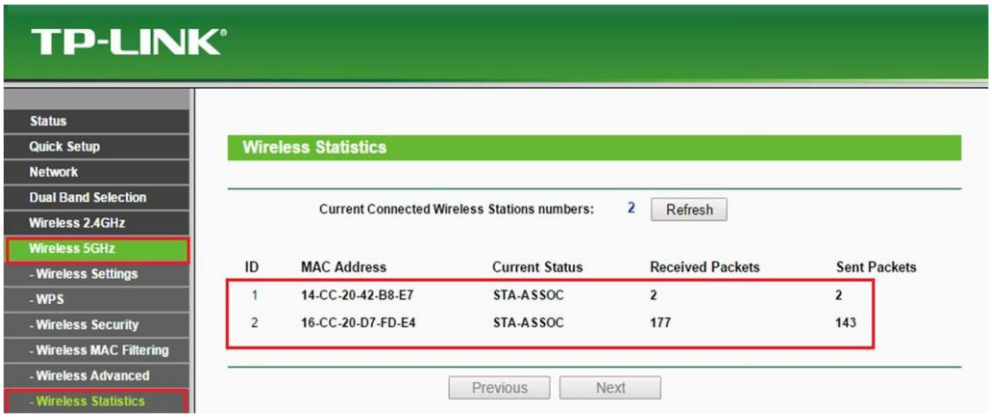
arxasında çap olunmuş MAC ünvanı ilə müqayisə edərək, 14-CC-20-42-B8-E5 MAC ünvanının gücləndiricinin 2.4 GHz tezliyində istifadə etdiyi MAC ünvanı olduğunu görəcəksiniz (şəkil 6.15).



Şəkil 6.15.

b. Əgər siqnal genişləndiriciniz iki diapazonlu gücləndiricidirsə, siz hələ də onun 5GHz MAC ünvanını tapmalısınız. Əvvəlki addımda olduğu kimi, siz 5GHz gücləndiricinizin MAC ünvanını asanlıqla tapa bilərsiniz (14-CC-20-42-B8-E7). Gücləndiricinin 2,4 GHz MAC ünvanı onun 5 GHz MAC ünvanına çox bənzəyir, əslində sonuncu oktada son iki simvolda fərqlənir.

Siqnal genişləndiricisinin 2,4 GHz MAC ünvanını (14-CC-20-42-B8-E5) 5 GHz MAC ünvanı (14-CC-20-42-B8 -E7) ilə müqayisə edərək nümunəni asanlıqla tapa bilərsiniz (şəkil 6.16).



Şəkil 6.16

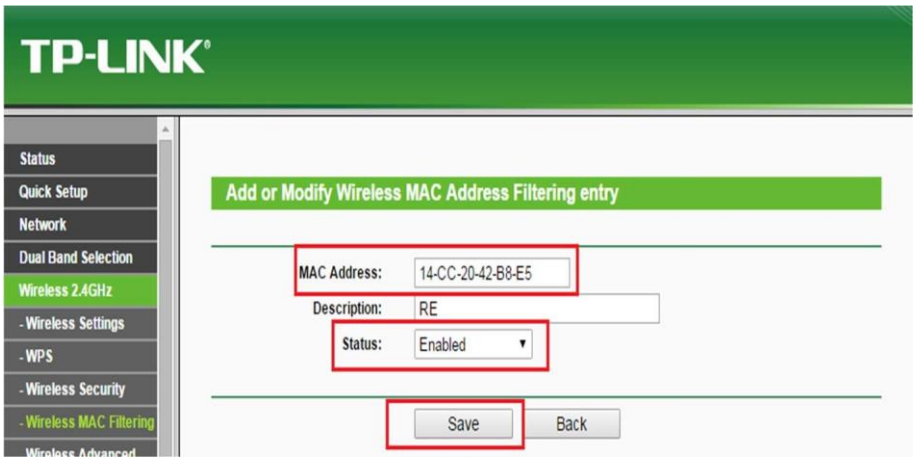
Qeyd: Routerinizin simsiz şəbəkə statistikasını necə yoxlamaq lazım olduğunu bilmirsinizsə, kömək üçün marşrutlaşdırıcı istehsalçınızla əlaqə saxlayın.

4. MAC ünvanları üzrə filtrləməni konfiqurasiyası (ağ siyahı): İnternetə çıxış üçün siyahıdan aktiv qaydalarda göstərilən stansiyalara girişə icazə verin. Bu nümunədə, MAC ünvan filtrini konfiqurasiya etmək üçün virtual MAC ünvanından necə istifadə olunacağını başa düşmək üçün Archer C7 modelində ağ siyahı konfiqurasiya edəcəyik (şəkil 6.17).

a. Routerin veb interfeysinə daxil olun və Simsiz 2.4GHz-> Simsiz Mac filtra ->Yeni əlavə et seçin. Sonra kompüterinizin Virtual MAC ünvanını daxil edin və Aktivləşdirildi->Saxla statusunu seçin.

Şəkil 6.17

b. Yenidən əlavə et üzərinə klikləyin və 2.4 GHz tezliyi üçün gücləndiricinizin MAC ünvanınıdaxil edin. Aktiv statusunu seçin->Saxla. (şəkil 6.17).



Şəkil 6.18

d. Əgər marşrutlaşdırıcınız və diapazon genişləndiriciniz iki diapazonlu cihazlardırsa, 5 GHz diapazonu üçün marşrutlaşdırıcının veb interfeysində yuxarıdakı addımları təkrarlaya bilərsiniz.

CİHAZIN YERLƏŞDİRİLMƏSİ QAYDASI VƏ SİQNAL GÜCÜ

Cihazın yerləşdirilməsi və siqnal gücü dedikdə simsiz şəbəkələrin təşkili və təhlükəsizliyi ilə bağlı məsələlər nəzərdə tutulur. Əsas ideya giriş nöqtələrinin siqnal gücünü elə tənzimləməkdir ki, onlar şəbəkə istifadəçiləri üçün istənilən ərazini əhatə etsin, lakin onun hüdudlarından kənara yayılmasın. Əsas məqsəd icazəsiz şəxslərin və ya cihazların simsiz şəbəkəyə daxil olmasının qarşısını almaqdır. Siqnal gücünün tənzimlənməsi şəbəkəni parolun təxmin edilməsi, məlumatların zəbt edilməsi və ya zərərli proqramların yeridilməsi kimi xarici hücumlara qarşı daha az həssas etməyə kömək edir. Bu, siqnal gücünü optimal şəkildə tənzimləməklə əldə edilir ki, bir bina və ya müəyyən bir ərazi daxilində rabitə təmin etmək üçün kifayətdir, lakin onun hüdudlarından kənara çıxmasın. Beləliklə, aşağı siqnal gücü onun aşkarlanması və kənardan şəbəkəyə daxil olmağa cəhd edə biləcək təcavüzkarlar tərəfindən istifadə edilməsi ehtimalını azaldır.

Cihazı simsiz şəbəkələr kontekstində yerləşdirmək üçün əsas qaydalar aşağıdakılardır:

1. Mərkəzi yer - Siqnalın bütün istiqamətlərdə bərabər paylanmasını təmin etmək üçün cihaz şəbəkənin əhatə dairəsinin mərkəzində yerləşdirilməlidir. Bu, zəif nöqtələri minimuma endirməyə və bütün istifadəçilər üçün daha yaxşı zəng keyfiyyətini təmin etməyə kömək edir.
2. Müdaxilədən mühafizə - Mümkün müdaxilənin və siqnalın pozulmasının qarşısını almaq üçün cihaz digər elektron cihazlardan və ya mikrodalğalı sobalar, simsiz telefonlar və ya CCTV sistemləri kimi müdaxilə mənbələrindən uzaqda yerləşdirilməlidir.
3. Yerləşdirmə hündürlüyü - Otaq konfiqurasiyasından asılı olaraq, ərazini ən yaxşı şəkildə əhatə etmək üçün cihaz müəyyən bir hündürlükdə quraşdırıla bilər. Məsələn, bir çox ofis binası optimal əhatə dairəsi üçün tavanda giriş nöqtələrinin quraşdırılmasını tövsiyə edir.
4. Müdaxilələrin aşkarlanması - Cihazı son yerləşdirməzdən əvvəl mümkün müdaxilə mənbələrini müəyyən etmək və bu təsiri minimuma

endirmək üçün optimal yeri seçmək üçün RF mühitinin hərtərəfli təhlilini aparmaq tövsiyə olunur.

5. Təhlükəsizlik - Cihazlar oğurlanma və ya zədələnmə riski olmayan təhlükəsiz yerlərdə quraşdırılmalıdır. Baxım və proqram yeniləmələrinin mövcudluğu da nəzərə alınmalıdır.

6. Fiziki maneələrin təyini - Divarlar, arakəsmələr və mebel kimi fiziki maneələr siqnalın yayılmasına təsir göstərə bilər. Cihazı yerləşdirərkən, onların mövcudluğunu və otağın quruluşunu nəzərə almaq lazımdır.

Bu prinsipləri nəzərə alaraq, cihazların simsiz şəbəkədə yerləşdirilməsi mümkün olan ən yaxşı əhatə dairəsini təmin etmək və siqnal keyfiyyəti ilə bağlı potensial problemləri minimuma endirmək üçün optimallaşdırıla bilər.

YOXLAMA SUALLARI

1. Simsiz təhlükəsizlik nədir və Wi-Fi şəbəkələri üçün nə üçün vacibdir?
2. Simsiz şəbəkələrdə istifadə olunan əsas təhlükəsizlik üsulları hansılardır?
3. Şifrələmə protokolları nədir və Wi-Fi şəbəkələrini qorumaq üçün necə istifadə olunur?
4. WEP, WPA və WPA2 kimi müxtəlif şifrələmə protokollarının üstünlükləri və çatışmazlıqları hansılardır?
5. MAC ünvan filtrasiyası nədir və Wi-Fi şəbəkələrini qorumaq üçün necə istifadə olunur?
6. Marşrutlaşdırıcılarda və giriş nöqtələrində hansı MAC ünvanlarının filtrasiya üsulları tətbiq oluna bilər?
7. DD-WRT nədir və simsiz şəbəkə təhlükəsizliyində hansı rol oynayır?
8. DD-WRT-də hansı təhlükəsizlik xüsusiyyətləri mövcuddur və mən onları Wi-Fi şəbəkələrimi qorumaq üçün necə konfiqurasiya edə bilərəm?
9. Cihazın yeri simsiz şəbəkə təhlükəsizliyinə necə təsir edir?
10. Siqnal gücünü optimallaşdırmaq və Wi-Fi şəbəkəsinə icazəsiz giriş risklərini minimuma endirmək üçün hansı üsullar və tövsiyələr var?

PRAKTİKİ TAPŞIRIQ

1. Ev istifadəsi üçün Wi-Fi şəbəkəsinin qorunmasının qurulması.

Tapşırıq: WPA2 protokolundan və güclü paroldan istifadə edərək ev Wi-Fi şəbəkənizi qurun. Routerinizdə MAC ünvan filtrini aktivləşdirin.

Məqsəd: Evinizin Wi-Fi şəbəkəsinin təhlükəsizliyini təmin edin və onu icazəsiz girişdən qoruyun.

2. Simsiz şəbəkə təhlükəsizliyi auditi.

Tapşırıq: Zəiflikləri aşkar etmək üçün xüsusi vasitələrdən istifadə edərək ofisdə Wi-Fi şəbəkəsinin təhlükəsizlik auditini aparın. Şifrələmə protokollarını, MAC ünvan filtrini və digər təhlükəsizlik üsullarını yoxlayın.

Məqsəd: Ofis şəbəkəsində zəiflikləri müəyyən etmək və korporativ məlumatların təhlükəsizliyini təmin etmək üçün onların aradan qaldırılması üçün planlar hazırlamaq.

3.Təhsil müəssisəsində təhlükəsiz simsiz şəbəkənin qurulması.

Tapşırıq: WPA2-Enterprise protokolundan istifadə edərək təhsil müəssisəsində Wi-Fi şəbəkəsi və RADIUS serverindən istifadə edərək autentifikasiya qurun. Yalnız müəyyən istifadəçi qruplarına girişə icazə verin.

Məqsəd: Təhsil müəssisəsində şəbəkə təhlükəsizliyini təmin etmək, icazəsiz girişin qarşısını almaq və tələbələrin və müəllimlərin məxfi məlumatlarını qorumaq.

4. İşçilərə simsiz şəbəkə təhlükəsizliyi üzrə təlim keçin.

Tapşırıq: Simsiz şəbəkələrdə təhlükəsizlik tədbirləri ilə bağlı işçilər üçün təlim seminarı təşkil edin. Şifrələmə protokollarını, MAC ünvanlarının filtrasiyasını, DD-WRT rollarını və müdaxilədən qorunma üsullarını müzakirə edin.

Məqsəd: Wi-Fi şəbəkəsi təhlükəsizliyi təhdidləri haqqında işçilərin məlumatlılığını artırmaq və onlara qorunma üsulları öyrətmək.

5. Xəstəxanada mobil cihazlar üçün simsiz şəbəkənin yerləşdirilməsi.

Tapşırıq: WPA2-Müəssisə protokolu və sertifikat autentifikasiyasından istifadə edərək xəstəxanada təhlükəsiz simsiz şəbəkə yerləşdirin. Müxtəlif kateqoriyalı istifadəçilər üçün şəbəkəni virtual seqmentlərə bölün.

Məqsəd: Heyət və xəstələrin mobil cihazları üçün tibbi məlumatlara və xəstəxana infrastrukturuna təhlükəsiz girişi təmin etmək.

MODUL 7. AUTENTİFİKASİYA, AVTORİZASİYA VƏ ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ

TƏHLÜKƏSİZLİK KONSEPSİYASI – AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)
AUTENTİFİKASİYA (DOĞRULAMA)
PAROL TƏHLÜKƏSİZLİYİ
AUTENTİFİKASİYA XİDMƏTLƏRİ
AVTORİZASİYA - GİRİŞƏ NƏZARƏT MODELLƏRİ
ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ
ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ ALƏTLƏRİ

YOXLAMA SUALLARI
PRAKTİK TAPŞIRIQ

TƏHLÜKƏSİZLİK KONSEPSİYASI AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)

"İçəridə düşmən olmayanda, xarici düşmənlər heç bir zərər verə bilməz."
Afrika atalar sözü

Təhlükəsizlik yeni problem deyil, o, bəşəriyyət yaranandan bəri mövcuddur və inkişaf etmişdir. Dolayı yolla, biz də öyrəndik ki, bir sistem interfeysi olan bir sərhəd kimi düşünülə bilər. Sərhəd bütövlüyü təmin olunarsa, təhlükəsizlik interfeysdən və onun vasitəsilə informasiya axınından asılı olacaq. Bu modulda biz sistem interfeysinə diqqət yetirəcəyik. Xüsusilə, təhlükəsiz interfeysi qorumaq üçün vacib olan üç komponentə baxacağıq. Bu komponentlərə daxildir: autentifikasiya, avtorizasiya və qeydiyyat.

Təhlükəsiz sistem qurmaq üçün biz yalnız səlahiyyətli şəxslərin müəyyən funksiyaları yerinə yetirə bilməsini təmin etməliyik. Xüsusilə, sistemimizdə icazə verilən subyektləri, obyektləri və hərəkətləri idarə edərək sistemimizi qorumalıyıq. Bu məqsədə çatmaq üçün autentifikasiya, avtorizasiya və auditin birləşməsi tələb olunur. Bu komponentlər bəzən AAA (Authentication, Authorization, and Accounting) təhlükəsizlik və ya təhlükəsizlik dünyasının üç başlı gözətçi iti adlanır.

Doğrulama subyektin müəyyən edilməsi prosesidir. Avtorizasiya subyektlər, hərəkətlər və obyektlər arasındakı əlaqələri müəyyən edir. İdentifikasiya subyektlərin obyektlər üzərində hərəkətlərinə nəzarət və ya yoxlama aktıdır. Bu üç komponent birlikdə bizə nəzarət etməyə və izləməyə imkan verir.

Təhlükəsizliyə bu baxışı belə ümumiləşdirmək olar: "Kim nəyi və nə vaxt edə bilər?" Doğrulama bizə "Kim"i müəyyən etməyə imkan verir. Avtorizasiya fəaliyyətə nəzarət edir ("nə etməli və nə vaxt etməli") və audit bütün hərəkətləri qeyd edir. Bir rəqəmsal sistemdə hər üç komponent lazımdır. Bir komponentin olmaması etibarsız bir sistemlə nəticələnə bilər. Bir komponentin uğursuzluğu bütün sistemi təhlükə altına ala bilər. Bu anlayışları təsvir etmək üçün aşağıdakı nümunələri nəzərdən keçirək.

Misal 1: Seyf.

Seyfin siyasəti ondan ibarətdir ki, açarı olan şəxsin seyfə daxil olmasına icazə verilir. Doğrulama açarın yoxlanılmasıdır. Bu halda, əsas yoxlama mexanizmi kiliddir. Qeyd, açarı kilidə daxil etmiş insanların qeydləri ola bilər.

Misal 2. ATM (Bankomat)

Avtomatlaşdırılmış kassa aparatı (ATM) bank işçisinə ehtiyac olmadan maliyyə əməliyyatlarının həyata keçirilməsinin təhlükəsiz üsulunu təmin edən kompüterləşdirilmiş sistemdir (qurğudur). Bu, yaxşı qurulmuş təhlükəsiz sistemin gözəl nümunəsidir. Doğrulama üçün sistem token (ATM kartı) və parol (şəxsi identifikasiya nömrəsi - PİN kod) birləşməsindən istifadə edir. Müştərilər maliyyə vəziyyətindən asılı olaraq müəyyən əməliyyatlar etmək hüququna malikdirlər. Əlavə olaraq istifadəçini izləmək üçün maşınla təchiz edilmiş bir video kamera, hər bir əməliyyat da bir günlük faylına qeyd olunur.

Misal 3. Şifrələmə.

Şifrələmə həm autentifikasiya, həm də avtorizasiya (bəzi proqramlarda) təmin edə bilən faydalı vasitədir. Şifrələmə açarı şifrələmə alqoritmi ilə birlikdə autentifikasiya mexanizmini təşkil edir; Hər bir şifrələmədə qurulmuş siyasət ondan ibarətdir ki, yalnız təsdiqlənmiş subyekt şifrələnmiş obyektə daxil ola bilər.

Mövzunun insanla məhdudlaşmaması heç bir əhəmiyyət kəsb etmir. Həqiqətən, obyektlər həm zaman, həm də məkan baxımından fərqlənə bilər. Məsələn, mövzu şəbəkə rabitəsində bir paket ola bilər. Paketi yaradan maşının arxasında həmişə bir adamın olduğunu iddia etmək olar. Lakin bu halda biz adama yox, paketə nəzarət edirik.

AUTENTİFİKASİYA (DOĞRULAMA)

"İnsanların ürəklərini deyil, üzlərini tanımaq asandır."
Çin atalar sözü

İstifadəçinin autentifikasiyası[34] şəbəkə daxilində təhlükəsizlik siyasətinin əsas komponentidir. Kompüter sistemində autentifikasiya istifadəçinin şəxsiyyətini yoxlama prosesidir. Doğrulamanın tərifləri müxtəlif kontekstlərdə

34

Əliquliyev R. M., İmamverdiyev Y.N. "İnformasiya təhlükəsizliyi insidentləri". Bakı - 2012, 219 s.
Əliquliyev R.M., İmamverdiyev Y.N.. Rəqəm imzası texnologiyası. Бакы: 2003, 130 s.
Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: 2006, 698 s.
Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. 2004. № 12.
Шрамко В. Я. Комбинированные системы идентификации и аутентификации / / PCWeek/RE. 2004. № 45.

fərqli ola bilər, lakin onların hamısı etibarlı, orijinal və ya etibarlı olma keyfiyyətinin və ya vəziyyətinin təsdiqlənməsi oxşarlığını bölüşür. İntuitiv olaraq, bir mövzunu yoxlamaq üçün bir işarənin yoxlanılması və ya subyektin özünün bəzi xüsusiyyətlərinin araşdırılması tələb olunur. Məsələn, tələbənin transkriptinin həqiqiliyini sənədin özündə universitet möhürünü yoxlamaqla yoxlaya bilərsiniz. Bu nümunədə əlamət universitet möhürüdür. Eynilə, şəxsin şəxsiyyəti həmin şəxsi (yaxud özünü) yoxlayaraq və ya taxdığı hər hansı bir şəxsiyyət nişanını yoxlayaraq təsdiqlənə bilər. Məsələn, Aysunun kimliyini yoxlamaq üçün yalnız Aysunun cavab verə biləcəyi sualdan istifadə edə bilərsiniz (məsələn, əvvəlcədən təyin edilmiş sual). Bu konsepsiya yeni deyil, (minlərlə) artıq neçə ildir mövcuddur. Bu, birinci Vyetnam Müharibəsi zamanı pilotların istifadə etdiyi siqnalla ən yaxşı şəkildə təsvir edilmişdir. Dolayı olaraq, biz subyektin əlamətinə və ya əmlakına etibar etməliyik, əks halda yoxlama prosesi mümkün olmayacaq. Tokenin autentifikasiyasının aşkar dezavantajı tokenin bütövlüyüdür. Məsələn, saxtakarlıq mümkün olsa belə, sürücülük vəsiqəsinin üzərində yazılmış şəxsin adının düzgün olduğuna inanmalıyıq. Bununla belə, identifikasiya üçün etibar lazımdır. Buna görə də, təkmilləşdirmə, autentifikasiya prosesini çoxlu token və ya xüsusiyyətlərə əsaslandırmaqdır. Bundan əlavə, biz də tokenlərin bütövlüyünü yoxlamalıyıq. Əgər autentifikasiya tokenlərə və ya subyekt xassələrinə əsaslanırsa, xassələri və ya tokenləri yoxlamaq üçün protokolları və metodları öyrənmək lazımdır. Əslində, onlar bu bölmənin ürəyidir. Köhnə tokenlərlə yanaşı, material smart tokenlər (məsələn, smart kartlar) konsepsiyasını da əhatə edəcək. Ümumiyyətlə, ağıllı tokenlər özlərini təsdiq edə bilən əlamətlərdir. Məsələn, smart kart şifrələnmiş açar və alqoritmdən ibarətdir. Biz sadə çağırış və cavab protokolundan istifadə edərək smart kartı yoxlaya bilərik.

Ümumiyyətlə, biz bir insanın bildiklərini yoxlamaqla, sahib olduğu nişanı yoxlamaqla və ya həmin şəxsin özünün dediyi şəxs olduğuna inanmaqla şəxsiyyətini təsdiq edə bilərik. Praktikada etimad anlayışına üçüncü şəxsin etibarı da daxildir. Məsələn, Tofiq onu dəstəkləsə, bu adamın Aysu olduğuna inana bilərik. Doğrulama metodunu seçərkən nəzərə alınmalı olan digər aspekt köçürmə qabiliyyətidir. Bəzi tokenlər asanlıqla başqa bir şəxsə ötürülə bilər, bəziləri isə keçə bilməz. Daşınmanın iki tərəfi var: həm arzu olunan, həm də arzuolunmazdır. Məsələn, bir insan öz işini edə bilməyəndə başqasından xahiş edə bilər. Bununla belə, köçürmə qabiliyyəti o deməkdir ki, token oğurlandıqda istifadə edilə bilər. Yaxşı bir bənzətmə ev açarıdır. Fiziki açardan nişanə kimi istifadə etməklə, sadəcə olaraq açarı onlara təhvil verməklə kiminsə evimizə

girməsinə asanlıqla icazə verə bilərik. Dezavantaj odur ki, biz təsadüfən açarı itirə bilərik və o, yanlış əllərə keçəcək. Əksinə, təsəvvür edin ki, evin qapısı ancaq sahibinin barmaq izi ilə açıla bilər, siz olmayanda (etibarlı) dostunuzdan evinizə baxmasını tələb etmək mümkün deyil. Bununla belə, tokeni idarə etməyə və izləməyə ehtiyac yoxdur. Məsələn, bir dostunuzun evinizə girməsinə icazə verə bilərsiniz, lakin o, açarı sonradan (zərərli) istifadə etmək üçün dublikat etməyəcəyinə zəmanət yoxdur. Məlumdur ki, tokenlər və xassələr subyektin şəxsiyyətini yoxlamaq üçün çox vacibdir. Bu o deməkdir ki, güclü autentifikasiyanın açarı tətbiq üçün uyğun nişanları və ya xassələri seçməkdir.

Autentifikasiya prosesində ən çox istifadə olunan üsullara aşağıdakılar daxildir:

- Paroldan istifadə
- Doğrulama nişanlarının (token) istifadəsi
- Biometrik məlumatların istifadəsi
- Çox faktorlu autentifikasiya

Paroldan istifadə - istifadəçi sistemdə saxlanan simvollarla müqayisə edilən unikal simvol birləşməsini (parol) daxil edir. Bu, ən çox yayılmış autentifikasiya üsullarından biridir.

Biometrik məlumatların istifadəsi üsulu istifadəçinin unikal fizioloji və ya davranış xüsusiyyətlərinə görə təyin olunur, məsələn, barmaq izləri, üz, səs və s.

Doğrulama nişanlarının (token) istifadəsi üsulu birdəfəlik parollar və ya istifadəçinin şəxsiyyətini təsdiqləmək üçün təqdim etməli olduğu digər kodları yaradan fiziki və ya virtual cihazlardır.

Çox faktorlu autentifikasiya üsulu təhlükəsizliyi yaxşılaşdırmaq üçün iki və ya daha çox müxtəlif autentifikasiya üsullarını (parol və biometrik məlumatlar kimi) birləşdirir.

Autentifikasiyanın əsas məqsədi yalnız düzgün istifadəçilərin lazımi resurslara daxil olmasını təmin etməklə sistemə və ya məlumatlara icazəsiz girişin qarşısını almaqdır. Nəzərə alın ki, hər bir autentifikasiya metodunun öz güclü və zəif tərəfləri var və ən mükəmməl autentifikasiya metodu yoxdur. Autentifikasiya metodları əsasən aşağıdakı 3 sualı cavablandırmağa xidmət edir:

- Nə bilirsiniz?
- Sənin nəyin var?
- Siz kimə güvənirsiniz?

Sən nə bilirsən? Bu sual parol və ya PIN kimi həssas məlumatları bilməklə bağlıdır. Bu suala əsaslanan üsullara parolların, gizli ifadələrin istifadəsi və təhlükəsizlik suallarının cavablandırılması daxildir.

Sənin nəyin var? Bu sual istifadəçinin şəxsiyyətini sübut etmək üçün təqdim edə biləcəyi fiziki və ya virtual obyektlərə aiddir. Bu autentifikasiya cihazı (token), smart kart, USB açarı və s. ola bilər.

Kimə güvənirsən? Bu sual hədəf sistem və ya resurs tərəfindən etibar edilən etibarlı qurumlara və ya sistemlərə aiddir. Çox faktorlu autentifikasiya, biometrik autentifikasiya və girişə nəzarət sistemləri bu aspekti həyata keçirə bilən üsullardır.

Sistemin kontekstindən və təhlükəsizlik tələblərindən asılı olaraq, istifadəçi təcrübəsinə minimal pozulma ilə ən yüksək səviyyədə təhlükəsizlik təmin etmək üçün müxtəlif autentifikasiya üsullarının kombinasiyası istifadə edilə bilər.

PAROL TƏHLÜKƏSİZLİYİ

İki nəfər arasındakı sirr Allahın sirridir, üç nəfər arasındakı sirr ümumidir.
İspan atalar sözü

Parollar[35] çox geniş istifadə edildiyindən və hücuma məruz qaldığından, çox diqqət parolların təhlükəsizliyinə yönəlib. Bura parol sındırma fayllarını qorumaq və istifadəçilərə parollarını idarə etməkdə kömək etmək daxildir.

Parol sındırma fayllarının qorunması. Şifrə sındırma fayllarının oğurlanmaması üçün serverlərin təhlükəsizliyini təmin etməklə yanaşı, tələlərin məzmununu qorumaq üçün əlavə tədbirlər görülə bilər. Bunlara salt istifadəsi və açarın uzanması daxildir. Salt Müəssisə üçün saxlanan parolları

35
https://blog.kaspersky.com/10-worst-password-ideas-as-seen-in-the-adobe-hack/3198/
http://lifehacker.com/5937303/your-clever-password-tricks-arent-protecting-you-from-todays-hackers
https://www.random.org/passwords/
http://world.std.com/~reinhold/diceware.html
https://www.safetydetectives.com/password-meter/
http://www.pcworld.com/article/2858642/you-can-encrypt-your-hard-drive-but-the-protection-may-not-be-worth-the-hassle.html
https://answers.syr.edu/display/software/Encrypting+your+external+hard+drive+on+Windows+and+OSX
http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946

qorumaq üçün vasitələrdən biri, hash alqoritmlərində istifadə olunan təsadüfi sətirdən ibarət salt əlavə etməkdir. Parollar bu təsadüfi sətri istifadəçinin açıq mətn paroluna hashing edilməmişdən əvvəl əlavə etməklə qoruna bilər. Salt çox sayda parolu sındırmaq üçün lüğət hücumlarını və kobud güc hücumlarını çətinləşdirir və göy qurşağı cədvəllərinin təsirini məhdudlaşdırır. Saltın başqa bir üstünlüyü odur ki, iki istifadəçinin eyni parolu seçməsi təcavüzkara kömək etmir. Salt olmadan, İstifadəçi №1-in parolunu sındıra bilən təcavüzkar heç bir hesablama aparmadan dərhal İstifadəçi №2-nin parolunu biləcək. Salt əlavə etməklə, lakin hər bir parol tələi fərqlidir.Bir insanın dediyi kimi olduğunu yoxlamağın bəlkə də ən asan yolu sual verməkdir, cavabını yalnız sistem və şəxs bilir.

Parol Zəiflikləri[36]. Şifrə zəiflikləri həqiqətən insan yaddaş məhdudiyyətləri və digər amillərlə bağlıdır. Parolun mürəkkəbliyi və idarə edilməsi ilə bağlı əsas problemlərə daxildir:

- Parolun mürəkkəbliyi və onların yadda saxlanması;
- Çoxsaylı hesabların mövcudluğu;
- Unikal parolların mövcudluğu;
- Parolun Müddətinin Bitməsi və Təhlükəsizlik Siyasətləri;
- Birdən çox cihazda parollar.

Araşdırmalara görə, ABŞ-da bir e-poçt ünvanında qeydiyyatdan keçmiş onlayn hesabların orta sayı 130-dur. Bir İnternet istifadəçisinə düşən hesabların orta sayının 207 olduğu təxmin edilir. Bir çox təhlükəsizlik siyasətləri parolların müəyyən bir müddətdən sonra, məsələn, hər 45-60 gündən bir yenisinin yaradılmalı olduğu zaman bitməsini tələb edir. Bəzi təhlükəsizlik siyasətləri hətta əvvəllər istifadə edilmiş parolun təkrar emal edilməsinin və yenidən istifadə edilməsinin qarşısını alır və istifadəçiləri dəfələrlə yeni parolları yadda saxlamağa məcbur edir.

Mürəkkəb və uzun parolları daha çox təhlükəsizlik təmin etməklə yanaşı, yadda saxlamaq daha çətindir. İstifadəçilər üçün hər hesab üçün unikal parollar tapmaq və yadda saxlamaq çətin ola bilər. İstifadəçilərin tez-tez müxtəlif veb-saytlarda və xidmətlərdə birdən çox hesabı olur. Çox sayda parolun idarə edilməsi çətin ola bilər. Təhlükəsizliyi artırmaq üçün hər bir hesab üçün unikal parollardan istifadə etmək tövsiyə olunur. Bununla belə, bir çox unikal parolları yadda saxlamaq daha da çətindir. Bəzi təşkilatlar parolların müntəzəm olaraq

[36] Port Checker - Check Open Ports Online (dnschecker.org)

dəyişdirilməsini tələb edir və həmçinin əvvəlki parolların təkrar istifadəsini qadağan edir. Bunun üçün daim yeni parolların yaradılması və yadda saxlanması tələb olunur ki, bu da yorucu ola bilər və daha az təhlükəsiz parollardan istifadə etməyə və ya onları yazmağa səbəb ola bilər. İstifadəçilər giriş üçün parol tələb edən kompüterlər, smartfonlar və planşetlər kimi bir çox cihazdan istifadə edə bilər. Bu, həmçinin parol idarə edilməsini çətinləşdirə bilər.

Təhlükəsizliyi artırmaq və istifadəçi təcrübəsini yaxşılaşdırmaq üçün parol menecerlərinin istifadəsi, iki faktorlu autentifikasiya, biometrik autentifikasiya üsulları və s. kimi müxtəlif yanaşmalar tətbiq oluna bilər. Bu alətlər insan yaddaşının məhdudiyyətlərini aradan qaldırmağa və parol idarəçiliyini sadələşdirməyə kömək edə bilər.

Zəif parolların geniş yayılması asanlıqla təsvir edilə bilər. 562 milyondan çox oğurlanmış parolun təhlili göstərdi ki, parolun ən çox yayılmış uzunluğu cəmi doqquz simvol, parolların 1 faizindən az hissəsi isə 14 simvoldan çox olub. Bundan əlavə, kiçik hərflərdən başqa simvollardan istifadə edən parolların faizi olduqca aşağı idi: böyük hərflər parolların yalnız 6 faizində, xüsusi simvollar isə yalnız 4 faizində tapılıb. Oğurlanmış 562 milyon parol içərisində ən çox yayılmış 10 parol çox zəifdir və Cədvəl 7.1-də verilmişdir.

Cədvəl 7.1.

Dərəcə	Parol
1	123456
2	123456789
3	abc123
4	password
5	password1
6	12345678
7	111111
8	1234567
9	12345
10	1234567890

Tanınmış bir təhlükəsizlik mütəxəssisi parol problemini aşağıdakıları ifadə edərək yaxşı ümumiləşdirdi: Problem ondadır ki, orta istifadəçi hücumların qarşısını almaq üçün kifayət qədər mürəkkəb parolları yadda saxlamağa belə cəhd edə bilmir və belə etməyəcək. Parollar nə qədər pis olsa

da, istifadəçilər onu daha da pisləşdirmək üçün əllərindən gələni edəcəklər. Onlardan parol seçməyi xahiş etsəniz, onlar pis parol seçəcəklər. Onları yaxşı birini seçməyə məcbur etsəniz, onu [aşağıya] yazacaq və onu keçən ay dəyişdirdikləri parola qaytaracaqlar. Və onlar bir neçə proqram üçün eyni parolu seçəcəklər.

Parol hücumları. Parollara edilən bəzi hücumlar təcavüzkarın giriş sorğusunda parolu "təxmin et" daxil etməsini əhatə etsə də, bu hücumların müvəffəqiyyət nisbəti aşağıdır. Bunun əvəzinə təcavüzkarlar yüksək müvəffəqiyyət nisbəti yaradan fərqli bir texnikadan istifadə edirlər.

İstifadəçi parol yaratdıqda, o, şifrələnməmiş açıq mətn formatında saxlanmır (və ya saxlanmamalıdır); bu, təcavüzkarların oğurlanmış parollardan istifadə etməsini çox asanlaşdıracaq. Bunun əvəzinə, birtərəfli hash alqoritmi parolun mesaj tələini (və ya hashını) yaradır. Bu tələ daha sonra orijinal açıq mətn parolu əvəzinə saxlanılır. İstifadəçi daha sonra daxil olmaq üçün parol daxil etdikdə daxil edilmiş paroldan tələ yaradılır. Bu digest saxlanılan tələlə müqayisə edilir və uyğun gələrsə, istifadəçinin autentifikasiyası aparılır. Təcavüzkarlar parol baza faylını oğurlamağa çalışırlar. Bu fayl təcavüzkarların əlinə keçdikdən sonra o, iki üsuldan birində istifadə edilə bilər. Bir üsul istifadəçini təqlid etmək üçün oğurlanmış hashdan istifadə etməkdir. Bu, parolları hədəf Windows maşınında saxlamaq üçün Microsoft Windows NTLM (Yeni Texnologiya LAN Meneceri) heşindəki boşluqdan istifadə etmək üçün tətbiq edilmişdir. NTLM parol bazasını oğurlaya bilən təcavüzkar sonrakı autentifikasiya üçün bu hashı uzaq sistemə göndərməklə istifadəçini təqlid edə bilər. Bu ötürmə hash hücumu kimi tanınır. Şifrə bazalarının oğurlanmış faylından daha geniş yayılmış istifadə, təhdid iştirakçılarının həmin faylı öz kompüterlərinə yükləmələri və sonra parolları sındırmaq üçün nəzərdə tutulmuş proqram təminatı olan mürəkkəb parol krakerindən istifadə etmələridir. Parol krakerləri məlum tələlər (namizədlər adlanır) yaradır və sonra onları oğurlanmış tələlərlə müqayisə edir. Uyğunluq baş verdikdə, təcavüzkar əsas parolu bilir. Parol krakerləri namizədlərin necə yaradıldığına görə fərqlənir. Namizədləri yaratmaq üçün bu müxtəlif vasitələrə kobud qüvvə, qayda, lüğət, göy qurşağı cədvəlləri və parol kolleksiyaları daxildir.

Parol spreyi (Password Spraying). Parol sındırımı faylını oğurlamağa cəhd etməyən bir parol hücumu əvəzinə bir növ "hədəflənmiş kobud güc"dən istifadə edir. Parol sprey hücumu bir və ya bir neçə ümumi parolu (Password1 və ya 123456) seçir və sonra birdən çox istifadəçi hesabına daxil olmağa cəhd edərkən eyni parolu daxil edir. Bu hədəf fərziyyə bir hesab üçün birdən çox

parol variantını sınamaqdansa, birdən çox hesaba şamil edildiyindən, həddən artıq uğursuz parol cəhdləri səbəbindən hər hansı həyəcan siqnalı vermək və ya istifadəçinin hesabını bloklamaq ehtimalı daha azdır. Parolla püskürtmə zaman zaman uğurlu ola bilsə də, hesabları sındırmaq üçün optimal vasitə hesab edilmir.

Sərt güc hücumu (Brute Force Attack). Avtomatlaşdırılmış sərt güc hücumu istifadəçinin parolunu müəyyən etmək üçün hərflərin, rəqəmlərin və simvolların istənilən mümkün kombinasiyasından istifadə edir. Hücum təsadüfi həyata keçirilmir, əksinə parolların yaradılmasına diqqətli yanaşmadan istifadə edir. Bir parolun birdən çox hesab üçün istifadə olunduğu parol sprey hücumundan fərqli olaraq, onlayn brute-force hücumunda eyni hesaba müxtəlif parollar daxil edilərək dəfələrlə hücum edilir (hücum adlanır). Bununla belə, onlayn kobud güc hücumları praktiki olmadığı üçün təcavüzkarlar tərəfindən nadir hallarda istifadə olunur. Saniyədə iki və ya üç cəhd olsa belə, düzgün parolu tapmaq minlərlə il çəkə bilər. Bundan əlavə, əksər hesablar məhdud sayda uğursuz cəhddən (məsələn, beş) sonra bütün girişləri deaktiv etmək üçün konfiqurasiya edilə bilər və təhlükəni dayandırır. Oflayn kobud güc hücumu oğurlanmış tələ faylı ilə başlayır. Təcavüzkar bu faylı kompüterə yükləyir və sonra hərflərin, rəqəmlərin və simvolların bütün mümkün kombinasiyalarından namizəd tələləri yaratmaq üçün parol sındırma proqramından istifadə edir. Namizədlər, uyğunluğu tapmaq üçün oğurlanmış tələ faylında namizədlərlə uyğunlaşdırılır. Bu, ən ləng, lakin ən güclü üsuldur.

Qaydalara uyğun hücum (Rule Attack). Qayda Hücumları, təcavüzkarın icazəsiz giriş və ya sui-istifadədən qorunmaq üçün sistemdə müəyyən edilmiş qaydalar və təhlükəsizlik siyasətlərini manipulyasiya etməyə və ya yan keçməyə çalışdığı bir hücum növüdür. Bu cür hücumlarda təcavüzkar qorunan resurslara giriş əldə etmək və ya müəyyən edilmiş nəzarətləri keçmək üçün qaydalardakı zəif cəhətlərdən və ya onların həyata keçirilməsindən istifadə edə bilər. Bu tip hücumlar tez-tez səhv konfiqurasiya edilmiş təhlükəsizlik qaydaları, qaydaların məntiqindəki qüsurlar və ya qaydalar bütün mümkün hücum ssenarilərini nəzərə almadığı üçün baş verir. Təcavüzkarlar bu boşluqlardan məlumat oğurlamaq, zərərli kod yeritmək və ya sistemlərə icazəsiz giriş əldə etmək kimi məqsədlərinə çatmaq üçün filtrləri, təhlükəsizlik duvarlarını və ya müdaxilənin qarşısının alınması sistemlərini yan keçmək üçün istifadə edə bilərlər. Qaydalara əsaslanan hücumlara qarşı effektiv müdafiə təhlükəsizlik qaydalarını mütəmadi olaraq nəzərdən keçirmək və sınaqdan keçirmək, onları yeni təhdidlərə görə yeniləmək və düzgün

konfiqurasiya edilməsini tələb edir. Qaydaları manipulyasiya etmək və ya keçmək cəhdlərini erkən mərhələdə aşkar etmək və mümkün hücumların qarşısını almaq üçün monitorinq və anomaliyaların aşkarlanması üsullarından istifadə etmək də vacibdir. Qaydalara görə hücum üç əsas mərhələdən ibarətdir:

1. Oğurlanmış parolu olan açıq mətn faylının kiçik bir nümunəsi tərtib olunur.

2. Cədvəl 7.1-də göstərildiyi kimi parolların uzunluğunu və simvol dəstlərini müəyyən etmək üçün nümunə üzərində statistik təhlil aparılır.

Cədvəl 7.1.

[*]	Length Statistics			
[+]		8:	62%	(612522)
[+]		6:	18%	(183307)
[+]		7:	14%	(146152)
[+]		5:	02%	(26438)
[+]		4:	01%	(15088)
[+]		3:	00%	(2497)
[+]		2:	00%	(308)
[+]		1:	00%	(113)
[*]	Charset Statistics			
[+]	Loweralphanum:		47%	(470580)
[+]	Loweralpha:		46%	(459208)
[+]	Numeric:		05%	(56637)

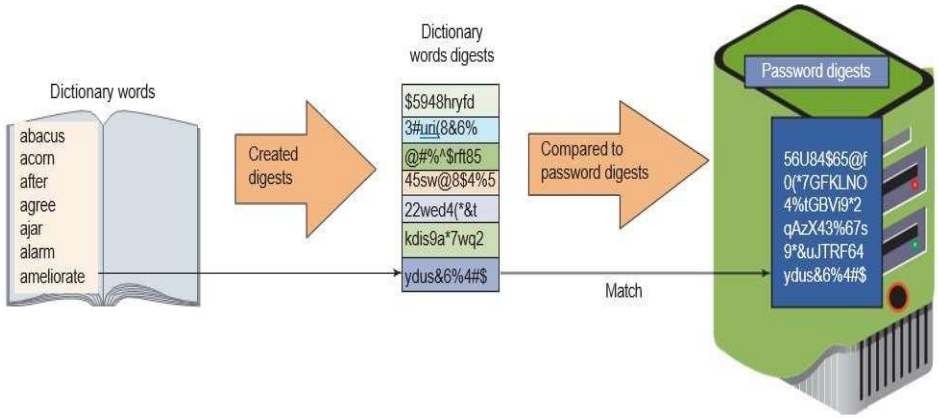
3. Parolların ən yüksək faizini sındırmaqda ən uğurlu olacaq bir sıra maskalar yaradılır.

Cədvəl 7.2

[*]	**Advanced Mask Statistics**		
[+]	?l?l?l?l?l?l?l?l:	04%	(688053)
[+]	?l?l?l?l?l?l:	04%	(601257)
[+]	?l?l?l?l?l?l:	04%	(585093)
[+]	?l?l?l?l?l?l?l?l:	02%	(516862)
[+]	?d?d?d?d?d?d?d:	03%	(487437)
[+]	?d?d?d?d?d?d?d?d?d?d:	03%	(478224)
[+]	?d?d?d?d?d?d?d?d:	02%	(428306)
[+]	?l?l?l?l?l?l?d?d:	02%	(420326)
[+]	?l?l?l?l?l?l?l?l?l:	02%	(416961)

[+]	?d?d?d?d?d?d:	02%	(390546)
[+]	?d?d?d?d?d?d?d?d:	02%	(307540)
[+]	?l?l?l?l?l?d?d:	02%	(292318)
[+]	?l?l?l?l?l?l?l?d?d:	01%	(273640)

Lüğət hücumu (Dictionary Attack). Başqa bir ümumi parol hücumu lüğət hücumudur. Lüğət hücumu təcavüzkarın namizədlər kimi ümumi lüğət sözlərinin tələlərini yaratması və sonra onları oğurlanmış tələ faylındakı sözlərlə müqayisə etməsi ilə başlayır. Lüğət hücumu şəkil 7.1-də göstərilmişdir. Lüğət hücumları uğurlu olur, çünki istifadəçilər çox vaxt sadə lüğət sözlərindən parol yaradırlar.



Şəkil 7.1. Lüğət hücumu (Dictionary Attack)

Lüğət sözlərindən istifadə edən və onu oğurlanmış tələlərlə müqayisə edən lüğət hücumu, məlum bir tələ (lüğət sözü) naməlum tələ (oğurlanmış tələ) ilə müqayisə olunduğu preimage hücumu kimi tanınır. Doğum günü hücumu bir az fərqlidir, çünki hər hansı iki eyni tələ axtarır. Lüğət hücumu və maska hücumunun birləşməsindən ibarət parol hücumuna hibrid hücum deyilir.

Açar uzatma. MD5 və SHA kimi ümumi təyinatlı hash alqoritmlərindən istifadə tələ yaratmaq üçün təhlükəsiz hesab edilmir, çünki bu hashing alqoritmləri mümkün qədər tez bir tələ yaratmaq üçün nəzərdə tutulub. Ümumi təyinatlı hash alqoritmlərinin sürəti təcavüzkarın xeyrinə işləyir. Təcavüzkar namizəd tələləri yaratdıqda, ümumi təyinatlı hashing alqoritmi uyğun məqsədlər üçün sürətlə çoxlu sayda parol yarada bilər. Parol tələlərini yaratmaq üçün daha təhlükəsiz bir yanaşma, qəsdən daha yavaş olmaq üçün

hazırlanmış xüsusi parol hash alqoritmindən istifadə etməkdir. Bu, təcavüzkarın parolları sındırmaq qabiliyyətini məhdudlaşdıracaq, çünki bu, hər bir namizəd tələini yaratmaq üçün əhəmiyyətli dərəcədə daha çox vaxt tələb edir və beləliklə, bütün krekinq prosesini ləngidir. Buna açarın uzanması deyilir. İki məşhur uzanan açar parolu hash alqoritmləri bcrypt və PBKDF2-dir. Bunlar tələ yaratmaq üçün daha çox vaxt tələb edəcək şəkildə konfiqurasiya edilə bilər. Şəbəkə administratoru parol hash funksiyasının nə qədər "bahalı" olacağını (kompüter vaxtı və/yaxud resurslar baxımından) təyin edən iterasiyaların (raundların) sayını təyin edə bilər.

Parolların idarə edilməsi. Parol sındırma faylları qorunmalı olsa da, fərdi istifadəçi parollarının təhlükəsiz saxlanması da vacibdir. Güclü parol üçün ən vacib amil mürəkkəblik deyil, uzunluqdur: daha uzun parol həmişə qısa paroldan daha təhlükəsizdir. Bunun səbəbi parol nə qədər uzun olarsa, təcavüzkar onu pozmaq üçün bir o qədər çox cəhd etməlidir. Mümkün parolların sayını müəyyən etmək üçün düstur yalnız iki elementi bilmək tələb edir: istifadə olunan simvol dəsti və parol uzunluğu.

Cədvəl 7.3-də standart 95 düyməli klaviaturadan istifadə edərək müxtəlif parol uzunluqları üçün mümkün parolların sayını və parolu pozmaq üçün lazım olan orta cəhdləri göstərir. Aydındır ki, daha uzun parolun sınıdırlmasına cəhd etmək qısa paroldan xeyli çox vaxt tələb edir. Lakin insan yaddaşının məhdudiyyətləri səbəbindən istifadəçilərin bütün hesablar üçün uzun, mürəkkəb və unikal parolları yadda saxlaması faktiki olaraq mümkün deyil. Parollar üçün insan yaddaşına etibar etmək əvəzinə, təhlükəsizlik mütəxəssisləri universal olaraq parolları saxlamaq və idarə etmək üçün texnologiyadan istifadə etməyi tövsiyə edirlər. Parolların təhlükəsizliyini təmin etmək üçün istifadə olunan texnologiyaya parol anbarları, parol açarları və aparat modullarından istifadə daxildir.

Cədvəl 7.3.

Klaviatura düymələri	Parol uzunluğu	Mümkün parolların sayı	Şifrəni sındırmaq üçün orta cəhdlər
95	2	9,025	4,513
95	3	857,375	428,688
95	4	81,450,625	40,725,313
95	5	7,737,809,375	3,868,904,688
95	6	735,091,890,625	367,545,945,313

Parol anbarları (password vaults) adından da göründüyü kimi, parol anbarı istifadəçilərin öz parollarını saxlaya biləcəyi təhlükəsiz anbardır. Parol meneceri kimi də tanınır, üç əsas növ mövcuddur:

1. Parol generatorları. Bunlar parol yaradan veb brauzer uzantılarıdır. İstifadəçi əsas parol daxil edir və parol generatoru əsas parola və veb saytın "tez" URL-nə əsaslanan parol yaradır. Parol generatorlarının dezavantajı odur ki, brauzer genişlənməsi hər bir kompüterdə və veb brauzerdə quraşdırılmalıdır.

2. Onlayn kassalar. Onlayn kassa istifadəçi parolunu yaratmaq əvəzinə veb brauzer uzantısından da istifadə edir. Hər dəfə o, parolu mərkəzi onlayn repozitoriyadan alır. Dezavantaj, parolları saxlayan onlayn saytların təcavüzkarlara qarşı həssas olmasıdır.

3. Parol idarəetmə proqramları. Parolun idarə edilməsi proqramı bir kompüterdə quraşdırılmış proqramdır. İstifadəçinin bir güclü əsas parol ilə qorunan bir istifadəçi "vault" faylında birdən çox güclü parol yarada və saxlaya biləcəyi yer. İstifadəçilər istifadəçi faylını açaraq lazım olduqda fərdi parolları əldə edə bilər və beləliklə, istifadəçini çoxsaylı parolları yadda saxlamaq ehtiyacından azad edir. Dezavantaj odur ki, proqram istifadəçi ilə aparılmalı və ya bir neçə kompüterdə quraşdırılmalıdır.

Parol açarları (Password keys). Kassaların zəif tərəfi onların proqram əsaslı olmasıdır ki, bu da onları zərərli proqramlara qarşı həssas edir. Parolları saxlamaq üçün daha təhlükəsiz aparat əsaslı həllər də mövcuddur. Onlara parol açarları deyilir. Şəkil 7.2-də parol açarını təsvir edir. Parol açarları çox vaxt aparat əsaslı parol meneceri, iki faktorlu təhlükəsizlik açarı və fayl şifrələmə cihazı kimi xidmət edir.

Şəkil 7.2. Parol açarı cihazı

Avadanlıq modulları kompleks kriptoqrafik aparat modulları parolların idarə edilməsini də asanlaşdıra bilər. Aparat təhlükəsizlik modulu (hardware security module - HSM) çıxarıla bilən xarici kriptoqrafik cihazdır. HSM USB cihazı, genişləndirmə kartı, port vasitəsilə birbaşa kompüterə qoşulan cihaz və ya təhlükəsiz şəbəkə serveri ola bilər. HSM-ə təsadüfi nömrələr generatoru və açar saxlama qurğusu, həmçinin sürətləndirilmiş simmetrik və asimmetrik şifrələmə daxildir və hətta həssas materialı şifrələnmiş formada ehtiyat nüsxəsini çıxara bilər. Kiçik istehlakçı yönümlü forma faktorunda HSM nümunəsi MicroSD HSM-dir. Təhlükəsiz Rəqəmsal (SD) kart kiçik forma faktorlu yaddaş daşıyıcısıdır və 1999-cu ildə yarandığı vaxtdan bir kart növü və ölçüsündən müxtəlif növ və ölçülərə qədər inkişaf etmişdir. SD formatına müxtəlif sürət dərəcələri ilə üç forma faktorunda mövcud olan dörd kart "ailəsi" daxildir. Hazırda SD kartların üç ölçüsü var: tam SD, miniSD və microSD. Tam SD yaddaş kartları adətən fərdi kompüterlərdə, video kameralarda, rəqəmsal kameralarda və digər böyük istehlak elektronikası cihazlarında istifadə olunur. MicroSD və miniSD kartlar adətən smartfonlar və planşetlər kimi kiçik elektron cihazlarda istifadə olunur. HSM ilə yanaşı, Etibarlı Platforma Modulu (Trusted Platform Module - TPM) kompüterin ana platasında kriptoqrafik xidmətlər göstərən çipdir. Məsələn, TPM PRNG əvəzinə əsl təsadüfi ədəd generatorunu, eləcə də asimmetrik şifrələmə üçün tam dəstəyi ehtiva edir və hətta ictimai və şəxsi açarlar yarada bilər.

Tək giriş. Bu gün istifadəçilərin üzləşdiyi problemlərdən biri, onların hər birinin unikal istifadəçi adı və paroldan istifadə etməli olduğu bir çox platformada çoxlu hesablarının olmasıdır. Fərqli autentifikasiya etimadnaməsini idarə etmək çətin olduğundan, istifadəçilər ən az ağır parol seçərək tez-tez güzəştə gedirlər və sonra onu bütün hesablar üçün istifadə edirlər. Bu problemin həlli bütün hesablara giriş əldə etmək üçün bir istifadəçi adı və parolun olmasıdır ki, istifadəçinin yadda saxlamaq üçün yalnız bir istifadəçi adı və parolu olsun. Bu, birdən çox şəbəkədə paylaşılan tək identifikasiya etimadnaməsini istifadə edən şəxsiyyət idarəçiliyinin arxasında duran ideyadır. Bu şəbəkələr müxtəlif təşkilatlara məxsus olduqda, bu, federasiya adlanır. Federasiyanın bir tətbiqi tək giriş (SSO) və ya birdən çox hesaba və ya tətbiqə daxil olmaq üçün bir identifikasiya etimadnaməsini istifadə etməkdir. SSO istifadəçilərin yadda saxlamalı olduğu istifadəçi adlarının və parolların sayını azaltmaq imkanına malikdir.

Kompüter sisteminə daxil olan istifadəçi sistemə daxil olarkən autentifikasiya[37] etimadnaməsini və ya identifikasiyasını təqdim etməlidir. İdentifikasiyanı təmin etmək üçün müxtəlif xidmətlərdən istifadə edilə bilər. Bunlara RADIUS, Kerberos, Terminal Girişinə Nəzarət Giriş İdarəetmə Sistemləri, kataloq xidmətləri, Təhlükəsizlik Təsdiqinin İşarələmə Dili və autentifikasiya çərçivə protokolları daxildir.

RADIUS və ya uzaqdan doğrulama istifadəçi xidməti (Remote Authentication Dial-In User Service (RADIUS)) mərkəzləşdirilmiş autentifikasiya, avtorizasiya və qeydiyyat üçün protokol və sistemdir və istifadəçinin təhlükəsiz girişini təmin etmək üçün tez-tez şəbəkələrdə istifadə olunur. RADIUS korporativ şəbəkələr, universitet şəhərcikləri və ya İnternet provayderi şəbəkələri kimi şəbəkə resurslarına daxil olmaq üçün istifadəçinin autentifikasiyasının tələb olunduğu mühitlərdə geniş istifadə olunur. RADIUS xidmətinin əsas komponentlərinə aşağıdakılar daxildir:

1. RADIUS server.
2. RADIUS müştəriləri.

RADIUS server istifadəçinin autentifikasiyası sorğularını emal edən və girişin verilməsi və ya rədd edilməsinə qərar verən mərkəzləşdirilmiş serverdir. O, həmçinin istifadəçilərə icazə verə və onların şəbəkə resurslarından istifadəsinə görə hesab verə bilər. RADIUS müştəriləri marşrutlaşdırıcılar, açarlar, giriş nöqtələri və şəxsiyyətlərini yoxlamaq və daxil olmaq üçün icazə almaq üçün istifadəçi identifikasiyası sorğularını RADIUS serverinə ötürən digər cihazlar kimi şəbəkə cihazlarıdır. RADIUS xidmətinin iş prinsipi şəkil 7.3-də təsvir olunmuşdur.

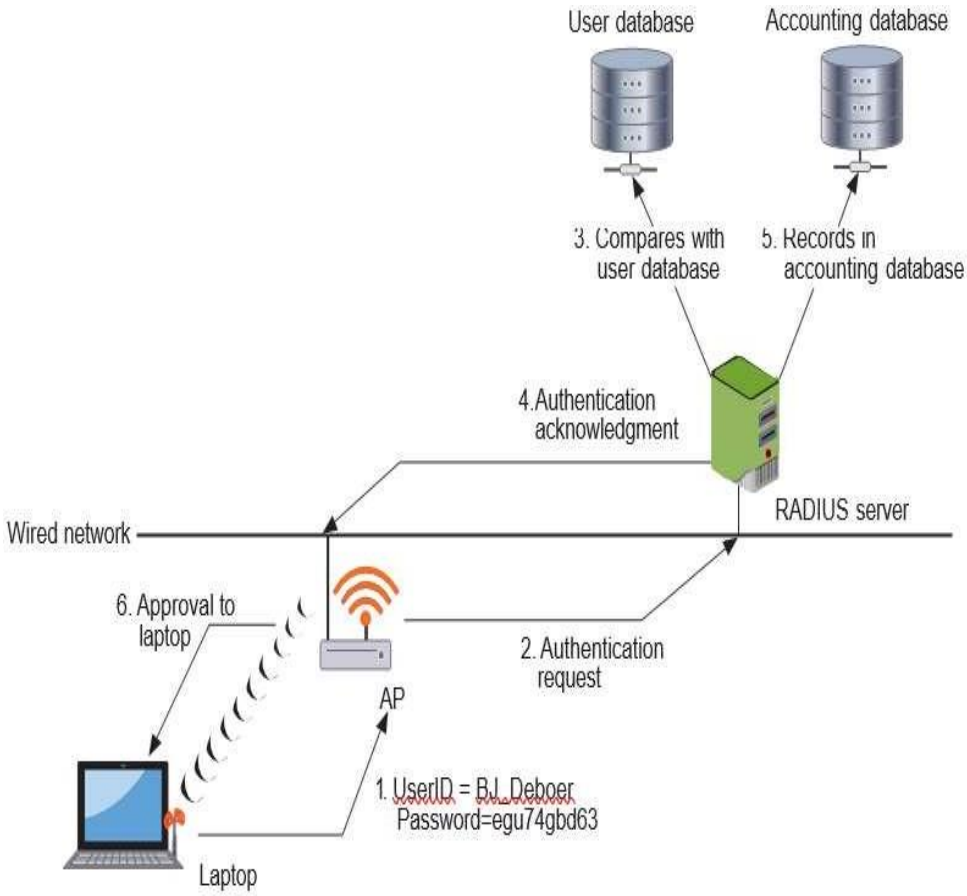
İstifadəçi, məsələn, simsiz şəbəkəyə qoşulmaqla və ya provayderin şəbəkəsinə daxil olmaq üçün nömrə yığmaqla şəbəkəyə daxil olmağa çalışır. Şəbəkə cihazı (müştəri) istifadəçinin etimadnaməsini (istifadəçi adı və parol kimi) RADIUS serverinə ötürür. RADIUS server istifadəçinin etimadnaməsini öz verilənlər bazası və ya xarici autentifikasiya mənbələri (məsələn, LDAP verilənlər bazası) ilə yoxlayır. Doğrulama nəticələrindən asılı olaraq RADIUS serveri istifadəçiyə giriş icazəsi vermək və ya rədd etmək barədə qərar qəbul edir. Əgər girişə icazə verilirsə, RADIUS serveri də avtorizasiya məlumatlarını

37

Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. 2004. № 12.

Шрамко В. Я. Комбинированные системы идентификации и аутентификации / / PCWeek/RE. 2004. № 45.

göndərə və şəbəkə resurslarından istifadə üçün qeydiyyat başlaya bilər. RADIUS şəbəkədə istifadəçi identifikasiyası və avtorizasiyasının mərkəzləşdirilmiş və çevik idarə edilməsini təmin edərək onu müxtəlif şəbəkə təhlükəsizliyi və girişə nəzarət ssenariləri üçün məşhur seçim halına gətirir.



Şəkil 7.3. RADIUS və ya Uzaqdan Doğrulama İstifadəçi Xidməti

Kerberos 1980-ci illərdə Massaçusets Texnologiya İnstitutu (MIT) tərəfindən hazırlanmış və şəbəkə istifadəçilərinin şəxsiyyətini yoxlamaq üçün istifadə edilən autentifikasiya sistemidir. Yunan mifologiyasında Cəhənnəm qapılarını qoruyan üç başlı (AAA) əjdaha adını daşıyan Kerberos təhlükəsizlik üçün şifrələmə və autentifikasiyadan istifadə edir. Kerberos Windows, macOS və Linux altında fəaliyyət göstərir. O, paylanmış şəbəkə mühitində müştərilərin və serverlərin etibarlı autentifikasiyası mexanizmini təmin edir. Kerberos-un

əsas məqsədi müştərilərin və resursların şəbəkənin müxtəlif qovşaqlarına

səpələnə biləcəyi paylanmış mühitdə autentifikasiya məlumatlarının ötürülməsi üçün təhlükəsizliyi təmin etməkdir. Kerberos sisteminin əsas komponentlərinə aşağıdakılar daxildir:

Kerberos açar dağıtım mərkəzi (Key Distribution Center- KDC).

Müştərilər və serverlər.

Kerberos Açar Dağıtım Mərkəzi (KDC) – müştərilərin və serverlərin autentifikasiyası üçün etibarlı üçüncü tərəf kimi çıxış edən mərkəzləşdirilmiş serverdir. KDC iki komponentdən ibarətdir:

1. Autentifikasiya server (Authentication Server - AS).

2. Bilet verən server (Ticket Granting Server -TGS).

Authentication Server (AS) müştəri etimadnaməsini təsdiq edir və onları müvəqqəti autentifikasiya nişanları ilə təmin edir. Ticket Granting Server (TGS) isə müştəriləri uğurlu autentifikasiyadan sonra Xidmət Biletləri ilə təmin edir.

Müştərilər və Serverlər müştərilər qorunan resurslara giriş tələb edən istifadəçilər və ya müştəri proqramlarıdır, serverlər isə istifadəçilərin daxil olmaq istədiyi resurslar və ya proqramlardır.

Kerberos autentifikasiyası prosesi adətən aşağıdakı addımları əhatə edir:

Müştəri etimadnamələrindən istifadə edərək Doğrulama Serverindən (AS) müvəqqəti bilet (TGT) tələb edir.

AS müştərinin etimadnaməsini yoxlayır və əgər onlar düzgündürsə, müştəri ilə KDC arasında paylaşılan açardan istifadə etməklə şifrələnmiş TGT yaradır və müştəriyə ötürür.

Müştəri Bilet Təqdimetmə Serverindən (TGS) xüsusi xidmətə giriş bileti (Xidmət Bileti) tələb etmək üçün TGT-dən istifadə edir.

TGS TGT-ni yoxlayır və əgər o etibarlıdırsa, müştərinin xidmətə autentifikasiya etmək üçün istifadə edə biləcəyi Xidmət Bileti yaradır və müştəriyə verir.

Müştəri xidmətin autentifikasiyası üçün Xidmət Biletindən istifadə edir və əgər xidmət bileti uğurla təsdiq edərsə, müştəriyə resurslara giriş imkanı verir.

Kerberos protokolu kriptoqrafiya və açar mübadiləsi prinsiplərindən istifadə etməklə autentifikasiya təhlükəsizliyini təmin edərək onu paylanmış şəbəkə mühitlərində ən populyar və təhlükəsiz autentifikasiya üsullarından birinə çevirir.

TACACS (Terminal Access Controller Access Control System) orijinal TACACS protokolu 1980-ci illərdə Cisco Systems tərəfindən hazırlanmışdır və RADIUS-a bənzər, UNIX cihazlarında ümumi istifadə edilən autentifikasiya xidmətidir və istifadəçi identifikasiyası məlumatını mərkəzləşdirilmiş serverə

yönləndirərək əlaqə saxlayır. O, istifadəçilərin autentifikasiyası və marşrutlaşdırıcılar və açarlar kimi şəbəkə cihazlarına girişi idarə etmək üçün istifadə edilmişdir. TACACS əsasən Cisco cihazlarında istifadə edilmiş və TCP protokolu üzərində işləmişdir. Bununla belə, o, məlumatların şifrələnməsini təmin etmədi, bu da onu dinləmələrə qarşı həssas etdi.

TACACS+ (Terminal Access Controller Access Control System Plus). Orijinal TACACS-in çatışmazlıqlarına cavab olaraq, TACACS+ protokolu 1990-cı illərin sonlarında hazırlanmış və buraxılmışdır. TACACS+, trafikin şifrlənməsini dəstəkləyən, daha təhlükəsiz autentifikasiya və avtorizasiyanı və təkmilləşdirilmiş audit imkanlarını təmin edən orijinal protokol üzərində əhəmiyyətli təkmilləşdirmə idi. TACACS+ Cisco mülkiyyət protokoludur və Cisco mühitlərində şəbəkə cihazlarına girişi idarə etmək üçün geniş istifadə olunur. TACACS sisteminin (TACACS+) əsas komponentlərinə aşağıdakılar daxildir:

- Müştərilər (Şəbəkə Qurğuları).
- TACACS Server (TACACS+ Server).
- İstifadəçi verilənlər bazası.
- Qeydlər və Hesabatlar.

Müştərilər (Şəbəkə Qurğuları) marşrutlaşdırıcılar, açarlar, autentifikasiya cihazları və şəbəkə resurslarına daxil olmaq üçün istifadəçilərin autentifikasiyası və avtorizasiyasını tələb edən digər avadanlıq kimi şəbəkə cihazlarıdır. TACACS Server (TACACS+ Server) müştərilərdən gələn autentifikasiya, avtorizasiya və mühasibat sorğularını emal edən mərkəzləşdirilmiş serverdir. TACACS serveri etimadnamələri yoxlamaq və şəbəkə resurslarına çıxışı təmin etmək üçün TACACS+ protokolundan istifadə edərək müştərilərlə əlaqə saxlayır. İstifadəçi verilənlər bazası istifadəçilər, onların etimadnamələri, icazələri və digər giriş parametrləri haqqında məlumatları ehtiva edən verilənlər bazasıdır. TACACS serveri autentifikasiya məlumatlarını yoxlamaq və avtorizasiya qərarları qəbul etmək üçün bu verilənlər bazasından istifadə edir. Qeydlər və Hesabatlar TACACS serveri hadisə qeydlərini saxlayır və uğurlu və uğursuz giriş cəhdləri, giriş sorğuları və digər şəbəkə fəaliyyəti daxil olmaqla istifadəçi fəaliyyəti haqqında hesabatlar təqdim edir. Bu, şəbəkə təhlükəsizliyini yoxlamağa və istifadəçi fəaliyyətini izləməyə kömək edir.

TACACS sisteminin (TACACS+) əsas komponentləri şəbəkə mühitlərində istifadəçilər üçün təhlükəsiz və çevik autentifikasiya, avtorizasiya və uçotu təmin etmək üçün birlikdə işləyir. Bu sistem şəbəkə resurslarına çıxışı

mərkəzləşdirilmiş şəkildə idarə etməyə və şəbəkə infrastrukturunun təhlükəsizliyini təmin etməyə imkan verir.TACACS (Terminal Access Controller Access Control System) və TACACS+ (Terminal Access Controller Access Control System Plus) protokollarında autentifikasiya prosesinin qısa təsviri aşağıdakı kimi yerinə yetirilir:

TACACS:

Müştəri autentifikasiya sorğusu göndərir (adətən marşrutlaşdırıcı və ya keçid kimi şəbəkə cihazına qoşulduqda).

TACACS serveri autentifikasiya sorğusunu qəbul edir və müştəridən istifadəçi adı və parol kimi etimadnamələri tələb edir.

TACACS serveri təqdim edilmiş etimadnamələri öz istifadəçi verilənlər bazası və ya xarici verilənlər bazası (məsələn, əməliyyat sistemi verilənlər bazası) ilə yoxlayır və onların etibarlı olub olmadığını müəyyən edir.

Etibarnamələri yoxladıqdan sonra TACACS serveri müştəriyə autentifikasiyanın uğurlu olub-olmadığını göstərən cavab göndərir.

TACACS+:

TACACS+-da autentifikasiya prosesi TACACS-dəki prosesə bənzəyir, lakin TACACS+ təkmilləşdirilmiş avtorizasiya və uçot imkanlarını da təmin edir.

Uğurlu autentifikasiyadan sonra TACACS+ serveri müştəriyə əlavə avtorizasiya məlumatları, məsələn, mövcud resursların siyahısı, giriş imtiyazları və istifadəçinin şəbəkə resurslarına çıxışını müəyyən edən digər parametrlər təqdim edə bilər.

TACACS+ həmçinin hadisə qeydi, audit və şəbəkə fəaliyyətinin hesabatı daxil olmaqla istifadəçi fəaliyyətinin izlənilməsini dəstəkləyir.

Həm TACACS, həm də TACACS+ protokolları mərkəzləşdirilmiş modeldən istifadə edir, burada TACACS serveri etimadnamənin yoxlanılmasını həyata keçirir və şəbəkə cihazlarına daxil olan istifadəçilər üçün autentifikasiya və avtorizasiya qərarları verir.

Təhlükəsiz təsdiq işarələmə dili (Security Assertion Markup Language - SAML) – təhlükəsiz veb domenlərinə istifadəçi identifikasiyası və avtorizasiya məlumatlarını mübadilə etməyə imkan verən XML standartıdır. Bu, istifadəçinin giriş etimadnaməsini hər bir veb-xidmət provayderinin serverində saxlamaq əvəzinə, tək identifikasiya provayderində saxlamağa imkan verir. SAML onlayn e-ticarət biznesdən biznesə (B2B) və biznesdən istehlakçıya (B2C) əməliyyatları üçün geniş şəkildə istifadə olunur.

SAML (Security Assertion Markup Language) sisteminin əsas komponentlərinə aşağıdakılar daxildir:

Şəxsiyyəti təyin edən provayderi (İdentity provayder - IdP).

Xidməti təyin edən provayder (Service Provider - SP).

SAML-nişan (token-Assertion).

SAML Metadata.

Şəxsiyyəti təyin edən provayder (İdentity provayder - IdP) istifadəçiləri autentifikasiya edən və SAML tokenləri şəklində autentifikasiya iddiaları verən SAML sistemin əsas komponentidir. IdP istifadəçinin autentifikasiyasını həyata keçirir və istifadəçinin şəxsiyyəti və atributları haqqında məlumat verir. IdP-lərə misal olaraq Windows və ya Okta, OneLogin və digər bulud SAML xidmətləri üçün Active Directory Federation Services (AD FS) kimi təşkilatın vahid autentifikasiya sistemini göstərmək olar.

Xidməti təyin edən provayder (Service Provider - SP) istifadəçinin autentifikasiyasını tələb edən və autentifikasiya və avtorizasiya məlumatlarını əldə etmək üçün SAML təsdiqlərindən istifadə edən veb proqram və ya xidmətdir. SP IdP-dən SAML təsdiqlərini qəbul edir və onlardan istifadəçilərin autentifikasiyası və resurslarına giriş icazəsi vermək üçün istifadə edir. SP-lərə misal olaraq e-ticarət veb proqramları, müəssisə portalları, bulud xidmətləri və digər onlayn resurslar daxildir.

SAML nişanı (Təsdiq) istifadəçinin autentifikasiyası və avtorizasiyası ilə bağlı iddiaları ehtiva edən XML sənədidir. Tokenə ID, atributlar və rollar kimi istifadəçi haqqında məlumat, həmçinin autentifikasiya, imza və etibarlılıq haqqında metadata daxildir. IdP və SP arasında təhlükəsiz əlaqəni təmin etmək üçün SAML tokenləri imzalana və şifrələnə bilər.

SAML metadatası SAML sisteminin konfiqurasiyası və parametrləri, o cümlədən IdP və SP URL-ləri, işarə formatları, sertifikatlar və digər parametrlər haqqında məlumatları ehtiva edir. Metadata IdP və SP arasında etibar yaratmaq və SAML sistemini avtomatik konfiqurasiya etmək və yeniləmək üçün istifadə olunur. Bu komponentlər müxtəlif veb domenləri arasında şəxsiyyət və imtiyaz məlumatlarının mübadilə edilməli olduğu paylanmış mühitlərdə təhlükəsiz istifadəçi autentifikasiyası və avtorizasiyasını təmin etmək üçün birlikdə işləyir.

SAML protokolunda autentifikasiya prosesi aşağıdakı addımları əhatə edir:

- Doğrulamanın başlanması.
- IdP-yə yönləndirmə.
- IdP-də doğrulama.
- Təsdiqlərin verilməsi (SAML nişanı).
- SP-yə geri yönləndirmə.

- SP-də SAML tokeninin yoxlanılması və işlənməsi.
- Avtorizasiya və girişin təmin edilməsi.

Doğrulamanın başlanması üçün istifadəçi Xidmət Provayderində (SP) mühafizə olunan resursa daxil olmağa çalışır. Məsələn, bu, veb portala daxil olmaq və ya onlayn xidmətdən istifadə etmək cəhdi ola bilər. SP istifadəçini İdentifikasiya Provayderinə (IdP) yönləndirir, autentifikasiya ehtiyacını göstərir və tələb olunan resurs haqqında məlumat verir (SP-nin təşəbbüsü ilə sorğu). İstifadəçi istifadəçi adı və parol kimi etimadnamələri təqdim etməklə IdP-yə autentifikasiya edir. IdP istifadəçinin autentifikasiya etimadnaməsini yoxlayır. Uğurlu autentifikasiyadan sonra IdP istifadəçinin autentifikasiyası ilə bağlı təsdiqləri ehtiva edən SAML nişanı (Təsdiq) yaradır. İddialara istifadəçi ID-si, atributlar, rollar və SP-yə autentifikasiya və avtorizasiya üçün tələb olunan digər məlumatlar daxil ola bilər. IdP SAML işarəsini ötürməklə istifadəçini yenidən SP-yə yönləndirir. SP-yə etibarlı ötürülməni təmin etmək üçün SAML tokeninə SP-yə istinad daxil edilmişdir. SP istifadəçidən SAML tokenini alır. SP, orijinallığını və bütövlüyünü təsdiqləmək üçün tokenin imzasını yoxlayır. SP həmçinin tokenin həmin xüsusi xidmət üçün verildiyini və tokenin istifadə müddəti bitmədiyini yoxlayır. SAML tokeninin uğurlu yoxlanılmasından sonra SP tokendə olan məlumatlar əsasında istifadəçiyə icazə verir. İstifadəçiyə tələb olunan resurs və ya xidmətə giriş hüququ verilir. Bu proses SAML standartından istifadə edərək müxtəlif veb proqramlar və xidmətlər arasında təhlükəsiz və səmərəli istifadəçi identifikasiyası və avtorizasiyanı təmin edir.

AVTORİZASİYA - GİRİŞƏ NƏZARƏT MODELLƏRİ

Dürüstlük ən yaxşı siyasətdir
İtalyan atalar sözü

İdentifikasiya[38] şəxsin şəxsiyyətini müəyyən etmək üçün kritik olsa da, Avtorizasiya onların şəxsiyyətinə əsaslanan sistemdəki insanlara və resurslara

38

Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011, 112 s.
Əliquliyev R. M., İmamverdiyev Y.N. "İnformasiya təhlükəsizliyi insidentləri". Bakı - 2012, 219 s.
Əliquliyev R.M., İmamverdiyev Y.N.. Rəqəm imzası texnologiyası. Бакы: 2003, 130 s.
Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: 2006, 698 s.
Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri»,

nəzarət etmək üçün vacibdir. Avtorizasiya sistemlə sıx bağlı olduğundan, ciddi şəkildə tətbiqdən asılıdır. Bu bölmə sistemin avtorizasiya prosesinin həyata keçirilməsi üçün çərçivə təqdim edir. Təhlükəsiz sistem həm də resursları yalnız qrant səlahiyyətinə malik olanlar tərəfindən istifadə edilməsinə icazə verməklə qorumalıdır.

İstehlakçılara və resurslara əsaslanan girişin məhdudlaşdırılması ümumiyyətlə Girişə Nəzarət adlanır. Giriş nəzarətini tətbiq etmək nəzəri cəhətdən sadədir (məsələn, bir neçə sətir kod kifayətdir). İstifadəçi autentifikasiya edildikdən sonra bu istifadəçinin daxil ola biləcəyi resurslara və funksiyalara nəzarət etmək üçün mexanizm tələb olunur. Sistemlər resurslara və istifadəçilərə görə fərqli olduğundan, icazə üçün ümumi yanaşma lazımdır. Fikri ümumiləşdirmək üçün prosesi iki hissəyə bölürük: Nəyə nəzarət etməli (Siyasət) və Necə nəzarət etməli (Növün icrası).

Avtorizasiya anlayışı müəyyən edilmiş istifadəçilərə əsaslanan sistemdə resurslara girişə nəzarət etmək üçün vacibdir. Avtorizasiyanın həyata keçirilməsi çox vaxt tətbiqlərə aid edilərək, giriş siyasətinin və ona aid nəzarət mexanizmlərini ehtiva edir. Giriş siyasəti konkret istifadəçilər və ya istifadəçi qrupları üçün hansı resursların mövcud olduğunu müəyyən edir. Buraya müxtəlif aspektlər daxil ola bilər, məsələn, giriş səviyyəsi (oxumaq, yazmaq, icra etmək), giriş vaxtı məhdudiyyətləri, qeyd səviyyəsində girişə nəzarət və s. Giriş siyasətləri çox vaxt rol modelinə əsaslanır, burada müxtəlif istifadəçi rollarına resurslara daxil olmaq üçün xüsusi imtiyazlar verilir. İstifadəçilər üçün istifadə imkanlarını qoruyarkən sistem təhlükəsizliyini təmin edəcək şəkildə giriş siyasətlərini tərtib etmək vacibdir.

Girişə nəzarət mexanizmləri isə siyasətlərin sistemdə necə həyata keçirildiyini müəyyən edir. Buraya müxtəlif istifadəçi autentifikasiyası üsulları (məsələn, parollar, biometrik məlumatlar), girişin yoxlanılması mexanizmləri (məsələn, girişə nəzarət siyahıları, təhlükəsizlik atributları) və girişin yoxlanılması və monitorinq mexanizmləri daxil ola bilər. Bəzi sistemlər mərkəzləşdirilmiş girişə nəzarət serverlərindən (giriş kataloqları və ya təhlükəsizlik siyasəti serverləri kimi), digərləri isə proqram və ya verilənlər bazası səviyyəsində yerli girişə nəzarət mexanizmlərini tətbiq edir.

Bakı, 2015.
Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.
Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.

Avtorizasiyaya ümumi yanaşma təhlükəsizlik və istifadənin lazımi səviyyəsini təmin etməklə yanaşı, sistemin xüsusi ehtiyaclarını və tələblərini nəzərə almalıdır.

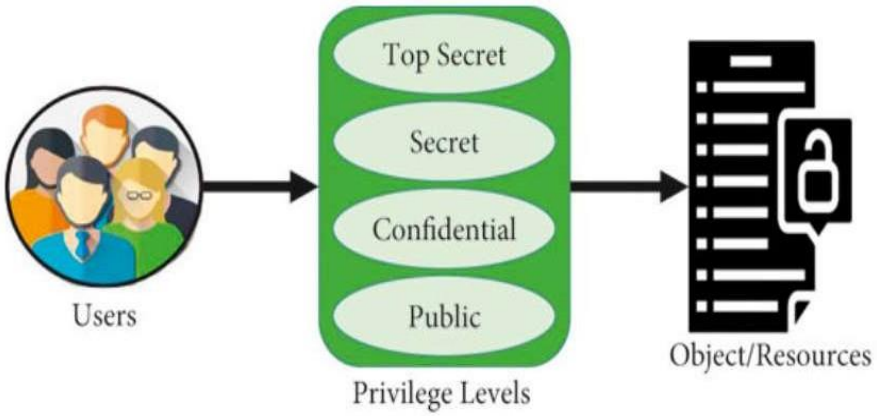
Girişə nəzarət modelləri informasiya sistemində resurslara girişin necə idarə olunduğunu müəyyən etmək üçün istifadə olunan metod və anlayışlardır. Onlar kimin hansı resurslara və nə qədər çıxışı olduğuna dair qərarların qəbul edilməsi qaydalarını və mexanizmlərini müəyyən edir. ən çox istifadə olunan girişə nəzarət modellərinə aşağıdakılar daxildir:

- Məcburi giriş nəzarəti (Mandatory Access Control - MAC)
- İxtiyari giriş nəzarət (Discretionary Access Control - DAC)
- Rol əsaslı giriş nəzarəti (Role-Based Access Control - RBAC)
- Atribut əsaslı giriş nəzarəti (Attribute-Based Access Control - ABAC)

Məcburi giriş nəzarəti (MAC) sistemdəki subyektlərə və obyektlərə təyin edilmiş məxfilik səviyyələrinə əsaslanır. Giriş qərarları sistem inzibatçısı tərəfindən müəyyən edilmiş rəsmi qaydalar və təhlükəsizlik siyasətləri əsasında qəbul edilir (şəkil 7.4).

Şəkildən göründüyü kimi, Məcburi Giriş Nəzarətinin (MAC) əsas komponentlərinə aşağıdakılar daxildir:

- Məxfilik Səviyyələri.
- Giriş matrisi.
- Təhlükəsizlik Siyasəti.
- Təhlükəsizlik Etiketləri.
- Qərar vermə mexanizmi.



Şəkil 7.4. Məcburi giriş nəzarəti (MAC)

MAC-da sistemdəki hər bir subyekt və obyektin məxfilik səviyyəsi var ki, bu da məlumatın məxfilik və ya həssaslıq dərəcəsini göstərir. Bu səviyyələr adətən rəqəm və ya hərf dəyərləri ilə təmsil olunur. Giriş matrisi subyektlərin sistemdəki obyektlərə giriş hüquqlarını əks etdirən cədvəldir. Matrisin hər bir elementi subyektə obyekt üzərində müəyyən bir hərəkət etməyə icazə verilib-verilmədiyini göstərir.

Təhlükəsizlik siyasəti hansı subyektlərin sistemdə hansı obyektlərə daxil olmaq hüququnu tənzimləyən qayda və qaydaları müəyyən edir. O, məxfilik və təhlükəsizlik qaydalarına uyğun olaraq məxfilik səviyyələrinin hansı birləşmələrinə icazə verildiyini və hansı girişə icazə verildiyini müəyyən edir. Təhlükəsizlik etiketləri sistemdəki hər bir mövzuya və obyektə əlavə edilmiş təhlükəsizlik məlumatıdır. Bu etiketlər subyektin və ya obyektin cari məxfilik səviyyəsi haqqında məlumatları ehtiva edir və təhlükəsizlik siyasətinə əsaslanan giriş qərarlarının qəbulu üçün istifadə olunur. Qərar mühərriki təhlükəsizlik siyasəti və təhlükəsizlik etiketləri əsasında subyektlərin hansı hərəkətlərinə icazə verildiyini və ya rədd edildiyini müəyyən edir. Bu, adətən, subyektin və obyektin təhlükəsizlik etiketlərini müqayisə edən və müəyyən qaydalar əsasında giriş qərarları verən alqoritmlər vasitəsilə həyata keçirilir. Bu komponentlər məcburi giriş nəzarəti olan sistemdə resurslara girişə səmərəli və təhlükəsiz nəzarəti təmin etmək üçün birlikdə işləyir.

Məcburi giriş nəzarəti (MAC) prosesi aşağıdakı addımları əhatə edir:

- Prosesin əvvəlində sistemdəki bütün subyekt və obyektlərə təhlükəsizlik səviyyələri təyin edilir. Bu səviyyələr məlumatın həssaslığını və ya həssaslığını göstərir.

- Sistemdəki hər bir subyekt və obyekt təhlükəsizlik səviyyələri haqqında məlumatı ehtiva edən təhlükəsizlik etiketləri ilə etiketlənir. Bu etiketlər adətən hər bir mövzuya və obyektə yapışdırılır.

-Təhlükəsizlik siyasəti hansı subyektlərin sistemdə hansı obyektlərə daxil olmaq hüququna malik olduğunu tənzimləyən qayda və qaydaları müəyyən edir. O, hansı təhlükəsizlik səviyyələrinin birləşməsinə icazə verildiyini və hansı girişə icazə verildiyini müəyyən edir.

-Sistemdəki obyektlərə subyektlərin giriş hüquqlarını göstərən giriş matrisi yaradılır. Matrisin hər bir elementi subyektə obyekt üzərində müəyyən bir hərəkət etməyə icazə verilib-verilmədiyini göstərir.

- Subyekt obyektə giriş tələb etdikdə qərar mühərriki subyektin və obyektin təhlükəsizlik etiketlərini təhlükəsizlik siyasəti ilə müqayisə edəcək.

Əgər giriş təhlükəsizlik siyasəti qaydalarına uyğundursa, ona icazə veriləcək, əks halda isə rədd ediləcək.

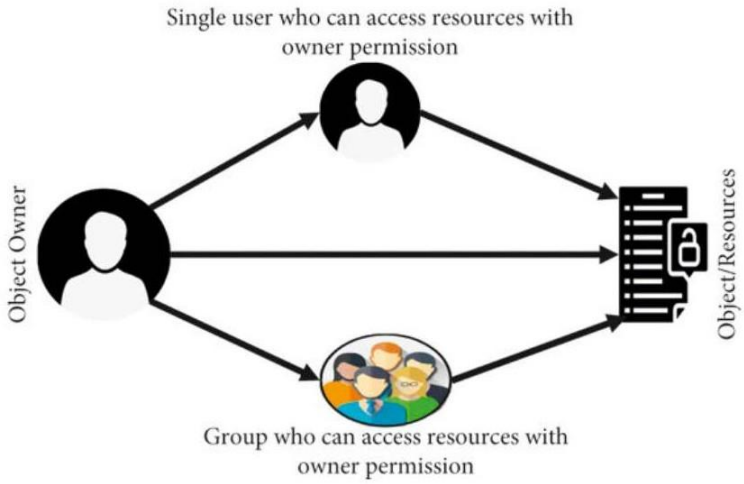
- Prosesin sonunda təhlükəsizlik siyasətlərinə uyğunluğu təmin etmək və potensial təhlükəsizlik pozuntularını müəyyən etmək üçün girişə nəzarət edilir və yoxlanılır.

Bu proses formal qaydalar və təhlükəsizlik siyasətləri əsasında sistemdəki resurslara çıxışa effektiv nəzarəti təmin edir.

İxtiyari girişə nəzarət (DAC) DAC resurs sahibləri tərəfindən təyin edilmiş giriş hüquqlarına əsaslanır. Resursun sahibi onun resurslarına kimin və nə dərəcədə daxil ola biləcəyinə tam nəzarət edir (şəkil 7.5). Discretionary Access Control (DAC) əsas komponentlərinə aşağıdakılar daxildir:

- Subyektlər və obyektlər.
- Giriş matrisi.
- Giriş hüquqları.
- Metadata təhlükəsizliyi.
- Qərar vermə mexanizmi.
- Resurs girişinə nəzarət.

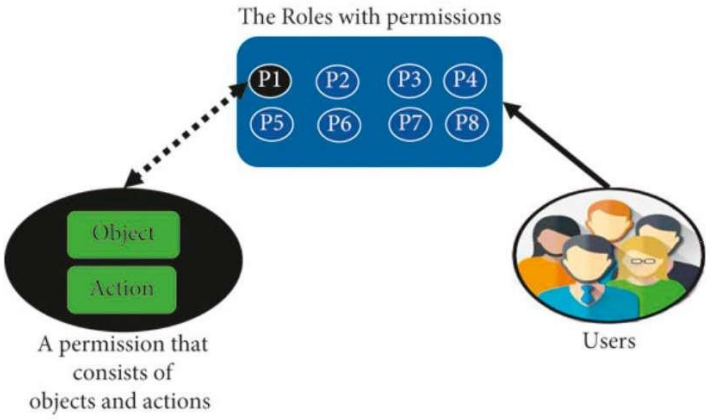
Subyektlər sistemdəki resurslara daxil olmağa çalışan istifadəçilər və ya proseslərdir. Obyektlərə isə fayllar, kataloqlar, qurğular və s. kimi giriş tələb olunan resurslar aiddir. Giriş matrisi subyektlərin sistemdəki obyektlərə giriş hüquqlarını əks etdirən məlumat strukturudur.



Şəkil 7.5. İxtiyari girişə nəzarət (DAC)

DAC-da matrisin hər bir elementi konkret subyektə və obyektə uyğundur və obyektə münasibətdə subyekt üçün hansı hərəkətlərə icazə verildiyini göstərir. Giriş hüquqları subyektin obyekt üzərində hansı hərəkətləri yerinə yetirə biləcəyini müəyyən edir. Bəzi ümumi icazələrə oxumaq, yazmaq, icra etmək və silmək daxildir. Giriş hüquqları obyektlər üzrə subyektlərə təyin edilə bilər və onlar konkret istifadəçilər və ya proseslər üçün hansı əməliyyatlara icazə verildiyini və ya rədd edildiyini müəyyən edir. Təhlükəsizlik metaməlumatları obyektlərə əlavə edilmiş və onların giriş hüquqlarını müəyyən edən məlumatdır. Adətən bu məlumat istifadəçilərin və ya istifadəçi qruplarının siyahısını və onların obyektə müvafiq giriş hüquqlarını ehtiva edir. DAC-da giriş qərarları obyektlərdə subyektlərə hansı giriş hüquqlarının təyin olunduğunu müəyyən edən qaydalar əsasında qəbul edilir. Bu qərarlar adətən əməliyyat sistemi və ya girişi idarə edən proqram modulları tərəfindən qəbul edilir. Girişə nəzarət giriş hüquqlarının təyin edilməsi və dəyişdirilməsi, həmçinin sistemdəki resurslara girişin idarə edilməsi proseslərini əhatə edir. İnzibatçılar məlumatların təhlükəsizliyini və məxfiliyini təmin etmək üçün subyektlərin obyektlərə giriş hüquqlarını idarə edə bilərlər. Bu komponentlər resurs sahibləri tərəfindən təyin edilmiş icazələrə əsaslanaraq sistemdəki resurslara girişə nəzarəti təmin etmək üçün birlikdə işləyir.

Rol əsaslı giriş nəzarəti (RBAC). RBAC resurslara giriş imtiyazları dəstini müəyyən edən istifadəçi rollarının təyin edilməsinə əsaslanır. İstifadəçilər xüsusi rollara təyin edilir və resurslara giriş həmin rollarla əlaqəli imtiyazlar əsasında verilir (şəkil 7.6).



Şəkil 7.6. Rol əsaslı girişə nəzarət (RBAC).

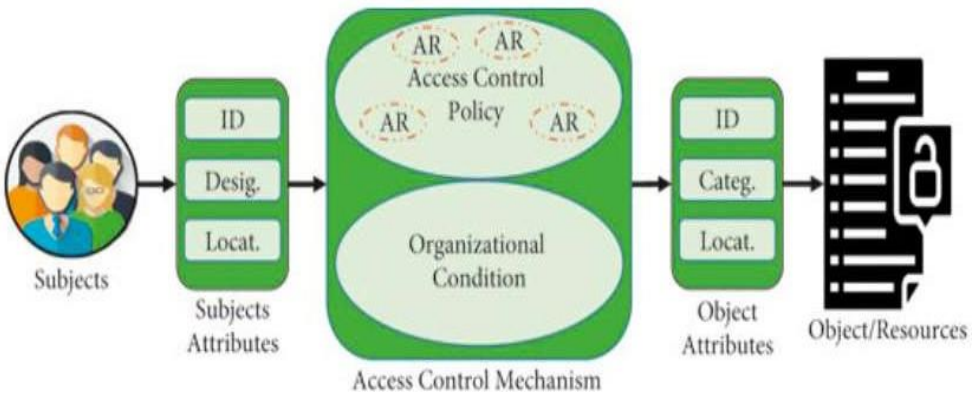
Rol əsaslı giriş nəzarətinin (RBAC) əsas komponentlərinə aşağıdakılar daxildir:

- Rollar.
- İstifadəçilər.
- İcazələr.
- İstifadəçilər və sistem arasındakı əlaqələr.
- Administratorlar və rol idarəetməsi.
- Təhlükəsizlik siyasəti və audit.

Rollar sistemdəki istifadəçilərin xüsusi funksiyaları və ya öhdəlikləri ilə əlaqəli giriş hüquqları toplusudur. Hər bir rolda istifadəçinin həmin rolun kontekstində yerinə yetirə biləcəyi icazə verilən hərəkətlər dəsti ola bilər.

İstifadəçilər sistemdən istifadə edən və onlara xüsusi sistem təyin edilə bilən şəxslər və ya qurumlardır.İstifadəçilər təşkilatdakı rollarından və ya məsuliyyətlərindən asılı olaraq bir və ya bir neçə rola təyin edilə bilər. İcazələr sistemdə hansı əməliyyatların və ya hərəkətlərin həyata keçirilə biləcəyini müəyyən edir. RBAC-da icazələr birbaşa istifadəçilərlə deyil, rollarla əlaqələndirilir. Yəni, hər rolun öz icazələri var.

Atribut əsaslı giriş nəzarəti (ABAC). ABAC subyektlərin, obyektlərin və digər kontekstual atributların atributlarına əsaslanır. Giriş siyasəti subyektlərin, obyektlərin və digər kontekst atributlarının atributlarının müəyyən qaydalara uyğunluğu əsasında müəyyən edilir. Hər bir modelin öz güclü və zəif tərəfləri var və konkret modelin seçimi konkret sistemin təhlükəsizlik və girişə nəzarət tələblərindən asılıdır (şəkil 7.7).



Şəkil 7.7. Atribut əsaslı giriş nəzarəti (ABAC)

Atribut əsaslı giriş nəzarətinin (ABAC) əsas komponentlərinə aşağıdakılar daxildir:

- Atributlar.
- Giriş Siyasəti.
- Qərar vermə mexanizmi.
- Atribut xidmətləri.
- Audit və monitorinq.
- Atributların həyat dövrünün idarə edilməsi.

Atributlar giriş qərarları qəbul etmək üçün istifadə olunan subyektlərin, obyektlərin və mühitlərin xüsusiyyətləridir.Atributlara istifadəçi haqqında məlumat (məsələn, rol, şöbə, etibar səviyyəsi), obyekt (məsələn, təsnifat, təhlükəsizlik etiketi) və kontekst (məsələn, giriş vaxtı, yer) daxil ola bilər.

Giriş siyasəti resurslara girişin verilməsi və ya məhdudlaşdırılması üçün qərarların qəbul edildiyi qayda və şərtləri müəyyən edir.Bu qaydalar subyektlərin, obyektlərin və kontekstlərin atributlarına, habelə onlar arasındakı əlaqələrə əsaslanır.

Qərar mühərriki giriş siyasətini qiymətləndirir və resursa girişə icazə verilib-verilmədiyini müəyyən etmək üçün subyekt, obyekt və kontekst atributlarını təhlil edir. Bu mexanizm təqdim edilmiş atributlar əsasında giriş şəraitini qiymətləndirən alqoritmlər və ya xidmətlər şəklində həyata keçirilə bilər.

Atribut xidmətləri subyektlərin, obyektlərin və kontekstlərin atributları haqqında məlumat mənbələridir. Bunlara şəxsiyyət kataloqları, identifikasiya və autentifikasiya idarəetmə sistemləri, girişə nəzarət cihazları və digər atribut mənbələri daxil ola bilər.

Audit və monitorinq mexanizmləri istifadəçi fəaliyyətlərini izləmək və qeyd etmək və sistemdəki qərarlara giriş üçün istifadə edilə bilər. Bu, təhlükəsizlik tələblərinə uyğunluğu, habelə insidentlərin təhlili və audit imkanlarını təmin etməyə kömək edir.

Atributların həyat dövrünün idarə edilməsi sistemdə atributların yaradılması, yenilənməsi və silinməsi proseslərini əhatə edir. Bu, giriş haqqında qərarlar qəbul etmək üçün istifadə olunan məlumatın cari və etibarlı olmasını təmin etmək üçün vacibdir. Bu komponentlər təhlükəsizlik siyasətinin dəyişən tələblərə və ətraf mühit kontekstinə uyğunlaşmasına imkan verən çevik və miqyaslı atribut əsaslı resurs girişinə nəzarəti təmin edir.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ

Şəbəkə təhlükəsizliyi auditi[39] zəiflikləri müəyyən etmək, anomal fəaliyyəti aşkar etmək və təhlükəsizlik siyasətlərinə uyğunluğu təmin etmək üçün şəbəkənin və onunla əlaqəli resursların təhlükəsizliyinin sistematik şəkildə qiymətləndirilməsi, təhlili və monitorinqi prosesidir. Şəbəkə təhlükəsizliyi auditinin əsas komponentlərinə aşağıdakılar daxildir:

- Zəifliyin qiymətləndirilməsi.
- Şəbəkə fəaliyyətinin monitorinqi.
- Doğrulama və girişə nəzarət.
- Nüfuz testi.
- Təhlükəsizlik siyasətlərinin təhlili.
- Sənədləşmə və hesabat.

Zəifliyin qiymətləndirilməsi konfiqurasiya, proqram təminatı və xidmətlər kimi müxtəlif aspektlərdə potensial zəiflikləri müəyyən etmək üçün şəbəkə və sistemlərin skan edilməsini nəzərdə tutur. Zəifliklər müəyyən edildikdən sonra hər bir zəifliklə bağlı risk səviyyəsi qiymətləndirilir və onların aradan qaldırılması üçün fəaliyyət planı hazırlanır. Bu proses şəbəkənizin təhlükəsizliyini təmin etmək və potensial təhlükələrdən qorunmaq üçün mühüm addımdır.

Şəbəkə və sistemləri skan edilməsi kompüterlər, serverlər, şəbəkə cihazları və digər resurslar kimi şəbəkədəki aktivləri müəyyən etməklə başlayır. Bu aktivlər daha sonra konfiqurasiya, proqram təminatı və xidmətlərdə zəiflikləri aşkar etmək üçün Nmap, OpenVAS və ya Nessus kimi xüsusi alətlərdən istifadə etməklə skan edilir. Tarama ya sorğular hədəf cihazlara göndərildikdə aktiv və ya şəbəkə trafiki və açıq portlar təhlil edildikdə passiv ola bilər.

Zəifliklər aşkar edildikdən sonra onların şəbəkənin və əlaqəli resursların təhlükəsizliyinə potensial təsiri qiymətləndirilir. Nəzərə alınan amillərə zəifliyin uğurlu istismarı ehtimalı, təhlükəsizlik pozuntusunun potensial nəticələri və mövcud əks tədbirlərin və təhlükəsizlik nəzarətlərinin

---

39

Сарбуков А.у Грушо А. Аутентификация в компьютерных системах // Системы безопасности. 2003. №5(53).
Семейство стандартов IEEE 802.11. http://www.wireless.ru/ wireless/wrl_base80211
Симонов С. В. Методология анализа рисков в информационных системах // Конфидент. 2001. № 1.
Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. Издательство Политехнического университета, Санкт-Петербург, 2005.

qiymətləndirilməsi daxildir. Riski qiymətləndirmək üçün tez-tez təhlükəsizlik pozuntusu ehtimalını və mümkün nəticələri nəzərə alan risk matrisi istifadə olunur.

Risklərin qiymətləndirilməsinə əsasən, dərhal aradan qaldırılması tələb olunan ən kritik zəiflikləri müəyyən etmək üçün zəifliklərə üstünlük verilir. Yalnız hər bir zəifliyin risk səviyyəsi nəzərə alınmır, həm də zəifliklərin aradan qaldırılması prosesinə təsir göstərə biləcək mövcud resurslar, vaxt qrafikləri və digər amillər nəzərə alınır. Bu zəifliyin qiymətləndirilməsi prosesi təşkilatlara müəyyən edilmiş zəifliklərlə bağlı risk səviyyəsini daha yaxşı başa düşməyə və şəbəkənin və əlaqəli resursların təhlükəsizliyini təmin etmək üçün lazımi bərpaedici tədbirləri görməyə imkan verir.

Şəbəkə fəaliyyətinin monitorinqi anomal nümunələri, şübhəli hadisələri və potensial təhlükəsizlik təhdidlərini aşkar etmək üçün şəbəkə trafikinin, şəbəkədə baş verən hadisələrin və fəaliyyətlərin davamlı olaraq təhlili və monitorinqi prosesidir. O, aşağıdakı aspektləri əhatə edir:

- Şəbəkə trafikinin monitorinqi.
- Hadisə jurnalının təhlili.
- Anomaliya aşkarlanması.
- Hadisəyə cavab.

Şəbəkə trafikinin monitorinqi qeyri-adi və ya gözlənilməz məlumat ötürmə nümunələrini müəyyən etmək üçün şəbəkə səviyyəsində trafikə nəzarət edir. Ümumi trafik həcminin, istifadə olunan protokolların, məlumat göndərənlərin və alıcıların təhlilini aparır.

Hadisə jurnalı anormal fəaliyyət və təhlükəsizlik hadisələrini müəyyən etmək üçün marşrutlaşdırıcılar, açarlar, firewalllar və serverlər kimi şəbəkə cihazlarının hadisə qeydlərinə nəzarət və təhlil edir. Monitorlar autentifikasiya cəhdləri, qadağan olunmuş resurslara giriş, hücumlar və digər şübhəli hadisələri uğursuz edir.

Anomaliya aşkarlanması qeyri-adi trafik sorğuları, qeyri-adi giriş cəhdləri və ya qeyri-adi resurs istifadə nümunələri kimi təhlükəsizlik təhdidlərinin mövcudluğunu göstərə bilən anormal davranış modellərini müəyyən edir. Şəbəkə fəaliyyətindəki anomaliyaları avtomatik aşkar etmək üçün maşın öyrənməsi və məlumat analitikası alqoritmlərindən istifadə edir.

Hadisəyə cavab aşkar edilmiş anomaliyaları və təhlükəsizlik hadisələrini araşdırmaq, bloklamaq və ya yumşaltmaq üçün tədbirlər görməklə cavab verir. Təhdidləri çevik idarə etmək və onların təsirini minimuma endirmək üçün avtomatlaşdırılmış insidentlərə cavab mexanizmlərinin tətbiqini reallaşdırır.

Şəbəkə fəaliyyətinin monitorinqi şəbəkə təhlükəsizliyinin təmin edilməsində əsas rol oynayır, potensial təhdidləri və hücumları tez müəyyən etməyə və onlara cavab verməyə, həmçinin arzuolunmaz hadisələrin və təhlükəsizlik insidentlərinin qarşısını almağa imkan verir.

Doğrulama və girişə nəzarət komponenti Doğrulama protokollarının, şifrələmə mexanizmlərinin təhlili, həmçinin girişə nəzarət mexanizmlərində zəifliklərin yoxlanılmasını əhatə edir. İstifadəçilərin autentifikasiyası və onların şəbəkədəki resurslara çıxışına nəzarət mexanizmlərinin qiymətləndirilməsi daxildir. Giriş qaydalarına və siyasətlərinə uyğunluğunun, onların müasir təhlükəsizlik standartlarına uyğunluğunun yoxlanılmasını əhatə edir.

Nüfuz testinin məqsədi hücumları simulyasiya etməklə və zəif nöqtələrdən istifadə etməklə şəbəkələrdə, sistemlərdə və tətbiqlərdə zəiflikləri müəyyən etməkdir. Sistemin real təhlükələrə qarşı müqavimətini qiymətləndirmək üçün ona nəzarət edilən hücumların həyata keçirilməsi planlaşdırır.

Təhlükəsizlik siyasətlərinə təşkilatın mövcud təhlükəsizlik siyasətlərinin və onların mövcud təhlükəsizlik standartlarına və tövsiyələrinə uyğunluğunun qiymətləndirilməsi daxildir. Məlumatların mühafizəsi siyasətlərinin, giriş siyasətlərinin və digər təhlükəsizlik qaydalarının effektivliyini yoxlayır. İnformasiya və şəbəkə resurslarının mühafizə səviyyəsinin yüksəldilməsi məqsədilə təhlükəsizlik siyasətinin təkmilləşdirilməsi üzrə tövsiyələrin hazırlanmasını təmin edir.

Şəbəkə təhlükəsizliyi auditinin nəticələri və aşkar edilmiş zəifliklər üzrə hesabatların hazırlanması daxil olmaqla, auditin mühüm mərhələsidir. Audit proseslərinin, istifadə olunan metodların, müəyyən edilmiş problemlərin və onların aradan qaldırılması üçün tövsiyələrin sənədləşdirilməsini əhatə edir. Müştərilərə və ya təşkilat rəhbərliyinə şəbəkə təhlükəsizliyinin cari vəziyyətini və onun təkmilləşdirilməsi üçün tövsiyələri təsvir edən hesabatları təqdim edir.

Bu komponentlər zəifliklər müəyyən etmək və aradan qaldırmaq, təhlükəsizlik siyasətlərinə uyğunluğu təmin etmək və real vaxt rejimində təhlükəsizlik təhdidlərinə cavab verməklə şəbəkənizin və əlaqəli resursların etibarlı şəkildə qorunmasını təmin etməyə kömək edir.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ AUDİTİ ALƏTLƏRİ

İstifadəçilərə və informasiya təhlükəsizliyi mütəxəssislərinə şəbəkənin təhlükəsizlik vəziyyətini qiymətləndirmək, zəiflikləri müəyyən etmək və təhlükəsizlik siyasətlərinə uyğunluğu təmin etmək üçün bir çox şəbəkə təhlükəsizliyi auditi alətləri mövcuddur. Ən məşhur alətlərə aşağıdakılar aid edilir:

- Nmap.
- OpenVAS.
- Wireshark.
- Metasploit.
- Snort.
- Nessus.
- Veb tətbiqi zəiflik skanerləri.
- SIEM platformaları.

Nmap şəbəkədəki cihazları aşkar etmək, açıq portları müəyyən etmək və zəiflikləri skan etmək üçün istifadə edilən güclü şəbəkə skaneridir. OpenVAS (Açıq Zəifliyin Qiymətləndirilməsi Sistemi) zəifliyin skan edilməsi və şəbəkə təhlükəsizliyinin təhlili üçün açıq platforma təqdim edir. Buraya zəifliklər haqqında məlumat bazası və təhlükəsizlik təhlili mexanizmləri daxildir. Wireshark şəbəkə trafikini tutmaq və təhlil etmək üçün istifadə edilən şəbəkə sniffer və protokol analizatorudur. Bu, şəbəkədəki anomaliyaları və hücumları müəyyən etməyə kömək edir.

Metasploit Framework şəbəkə sistemlərinə idarə olunan hücumların həyata keçirilməsi üçün bir sıra istismar və alətləri özündə cəmləşdirən məşhur nüfuz sınağı alətidir. Snort şəbəkə trafikinə nəzarət etmək və real vaxt rejimində anomal fəaliyyət və hücumları aşkar etmək üçün istifadə edilən müdaxilənin aşkarlanması sistemidir (IDS). Nessus zəifliyin aşkarlanması və şəbəkə təhlükəsizliyinin təhlili üçün geniş spektrli funksiyalar təqdim edən kommersiya zəifliyinin skan edilməsi vasitəsidir. Veb tətbiqi zəiflik skanerləri Burp Suite, OWASP ZAP, Acunetix kimi veb proqramlardakı boşluqların aşkarlanmasında ixtisaslaşan bir çox veb proqram zəifliklərinin skan edilməsi alətləri mövcuddur. SIEM platformaları (Hadisə və informasiya təhlükəsizliyi idarəetmə sistemləri) Splunk, IBM Qradar, ArcSight kimi SIEM platformaları təhdidləri və anomaliyaları aşkar etmək üçün şəbəkə təhlükəsizliyi hadisələrinin toplanması, təhlili və monitorinqi üçün güclü alətlər təqdim edir.

Bu, şəbəkə təhlükəsizliyi auditi üçün mövcud olan alətlərin kiçik siyahısıdır. Onların hər biri öz xüsusiyyətlərinə malikdir və xüsusi şəbəkə təhlükəsizliyi tapşırıqlarını yerinə yetirmək üçün nəzərdə tutulmuşdur. Beləliklə, şəbəkə təhlükəsizliyi auditləri şəbəkəni potensial məlumat pozuntularından və kiberhücumlardan qorumaq üçün zəruridir. Şəbəkə təhlükəsizliyi auditi və ya şəbəkə təhlükəsizliyinin qiymətləndirilməsi rəsmi təhlükəsizlik nəzarəti təhlili və ya sizin və müştərilərinizin məlumatlarını və həssas məlumatlarını qorumaq üçün istifadə edilən sistemdir.

YOXLAMA SUALLARI

1. AAA (Authentication, Authorization, Accounting) təhlükəsizlik konsepsiyası nədir və şəbəkə təhlükəsizliyi üçün hansı üstünlükləri təmin edir?
2. Şəbəkə təhlükəsizliyində autentifikasiya (yoxlama) prosesinin əsasında hansı əsas prinsiplər dayanır?
3. Təhlükəsizlik parolu nədir və onu yaratmaq və saxlamaq üçün hansı üsullardan istifadə olunur?
4. Şəbəkələri qorumaq üçün hansı autentifikasiya xidmətləri mövcuddur və onlar necə işləyir?
5. Şəbəkədəki istifadəçiləri və cihazları avtorizasiya etmək üçün hansı girişə nəzarət modellərindən istifadə olunur?
6. Şəbəkə təhlükəsizliyi auditi nədir və şəbəkələrinizi təhlükəsiz saxlamaq üçün nə üçün vacibdir?
7. Şəbəkə təhlükəsizliyi auditinin aparılması üçün hansı vasitələrdən istifadə olunur və onlar hansı vəzifələri yerinə yetirirlər?
8. Şəbəkə infrastrukturunda təhlükələri və pozuntuları müəyyən etmək üçün hansı audit məlumatlarının təhlili üsullarından istifadə edilə bilər?
9. Şəbəkə təhlükəsizliyində müxtəlif autentifikasiya və avtorizasiya üsullarının üstünlükləri və çatışmazlıqları hansılardır?
10. Şəbəkə təhlükəsizliyinin autentifikasiyası və audit məlumatlarının qorunması üçün hansı təhlükəsizlik tədbirləri görülə bilər?

PRAKTİKİ TAPŞIRIQ

1. Ofis şəbəkəsində çoxfaktorlu autentifikasiyanın qurulması.

Tapşırıq: Korporativ şəbəkəyə daxil olmaq üçün çoxfaktorlu autentifikasiya sistemini qurun. İstifadəçilərin autentifikasiyası üçün parol və işarənin istifadəsini aktivləşdirin.

Məqsəd: Korporativ məlumatları icazəsiz girişdən qorumaq üçün əlavə təhlükəsizlik səviyyəsini təmin etmək.

2.Veb tətbiqi təhlükəsizlik auditi.

Tapşırıq: SQL injection, XSS və CSRF hücumları kimi zəiflikləri aşkar etmək üçün xüsusi vasitələrdən istifadə edərək veb proqram təhlükəsizlik auditini aparın.

Məqsəd: Veb tətbiqində potensial zəiflikləri müəyyən edin və zərərli istifadəçilər tərəfindən mümkün hücumların qarşısını almaq üçün onları aradan qaldırmaq üçün tədbirlər həyata keçirin.

3. Routerdə ACL-in həyata keçirilməsi.

Tapşırıq: Şəbəkədəki müəyyən resurslara və ya xidmətlərə girişə icazə vermək və ya rədd etmək üçün marşrutlaşdırıcıda girişə nəzarət siyahılarını (ACL) konfiqurasiya edin.

Məqsəd: Şəbəkə resurslarına girişi idarə etmək və təcavüzkarların zəifliklərdən istifadə etmək imkanlarını məhdudlaşdırmaq.

4.Server təhlükəsizliyi auditi.

Tapşırıq: Quraşdırılmış proqramları, açıq portları, yeniləmələri və təhlükəsizlik parametrlərini yoxlamaq daxil olmaqla server təhlükəsizliyi auditini aparın.

Məqsəd: Potensial server zəifliklərini və təhlükəsizlik pozuntularını müəyyən edin və server məlumatlarını və proqramlarını qorumaq üçün bərpa planı hazırlayın.

5.Bulud yaddaşında məlumatların şifrələmə mexanizmlərinin tətbiqi.

Tapşırıq: məxfi məlumatları icazəsiz girişdən qorumaq üçün bulud yaddaşında məlumatların şifrələmə mexanizmlərini qurun.

Məqsəd: Buludda ötürülən və saxlanılan məlumatların məxfiliyini təmin etmək və mümkün məlumat sızmasının qarşısını almaq.

MODUL 8. ÜMUMİ TƏHDİDLƏR VƏ ZƏİFLİKLƏR

MƏXFİLİK, TAMLIQ VƏ ƏLÇATANLIĞA YÖNƏLMİŞ TƏHDİDLƏR
Wİ-Fİ ZƏİFLİKLƏRİ
ŞƏBƏKƏ CİHAZI ZƏİFLİKLƏRİ
TƏHLÜKƏSİZLİK TƏHDİDLƏRİ VƏ RİSKLƏRİ
ETİBARLILIQ VƏ KİMLİYİN İDARƏ OLUNMASI

YOXLAMA SUALLARI
PRAKTİK TAPŞIRIQ

MƏXFİLİK, TAMLIQ VƏ ƏLÇATANLIĞA YÖNƏLMİŞ TƏHDİDLƏR

Şəbəkə təhlükəsizliyi ümumi biznes prosesləri mexanizmləri çərçivəsində fəaliyyət sektorlarında risklərin idarə edilməsi üzrə öhdəliklərinin bir hissəsidir. Hər bir sektor əslində korporativ aktivlərin dəyərinə əsaslanan məqbul risk və zəiflik səviyyələrini müəyyən etməlidir. Müəssisələr həmçinin risk ehtimalını və təhlükəsizliyin pozulması halında kəmiyyətcə ölçülə bilən zərərin ağlabatan gözləntilərini müəyyən etməlidirlər. Risklərin idarə edilməsinin bu aspekti risklərin qiymətləndirilməsi adlanır və bu, təşkilatların yazılı təhlükəsizlik siyasətlərinin əsas hərəkətverici qüvvəsidir. Şəbəkə dizaynerləri və mühəndisləri bu təhlükəsizlik siyasətlərinin hazırlanmasında əsas rol oynayırlar; lakin bu, təhlükəsizliyin həyata keçirilməsi mərhələsinə şamil edilmir.

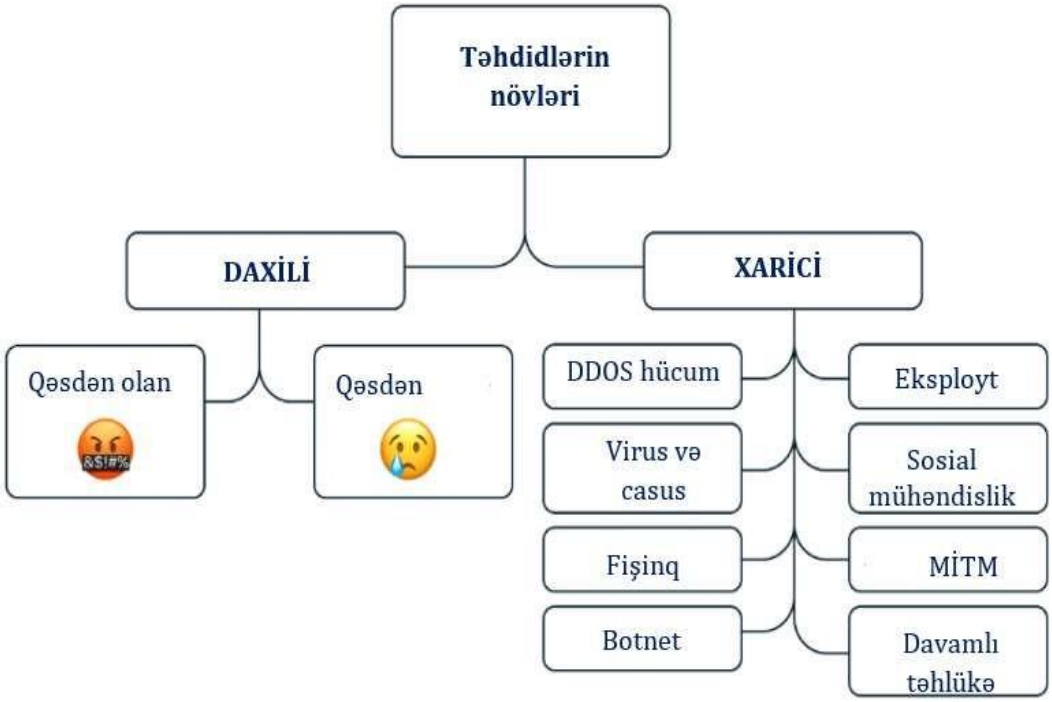
Şəbəkə mühəndisi hücumun tanınması və bu xüsusi hücumlar üçün əks tədbirlərin müəyyən edilməsi prosesində olduqda, o, ən pis vəziyyətləri nəzərdən keçirməli və planlaşdırmalıdır, çünki müasir şəbəkələr böyükdür və onlar bir çox təhlükəsizlik təhdidlərinə həssas ola bilər. Bu təşkilatlardakı proqramlar və sistemlər çox vaxt çox mürəkkəbdir və bu, xüsusilə şirkət Veb proqramları və xidmətlərindən istifadə etdikdə onları təhlil etməyi çətinləşdirir. Bu üç atribut müəssisənin təhlükəsizlik siyasətinin əsasını təşkil edir. Məxfilik yalnız səlahiyyətli istifadəçilərin, tətbiqlərin və ya xidmətlərin həssas məlumatlara daxil ola bilməsini təmin edir. Dürüstlük məlumatların icazəsiz istifadəçilər və ya xidmətlər tərəfindən dəyişdirilməməsini nəzərdə tutur. Nəhayət, sistemlərin və məlumatların mövcudluğu hesablama resurslarına fasiləsiz çıxışın olmasını təmin etməlidir.

Təhdidlərin növləri[40]. İnformasiya təhlükəsizliyi sahəsində qəbul edilmiş meyarlara uyğun olaraq təhdidlər daxili və xarici olmaqla 2 qrupa ayrılır. Təhdidlərin növləri şəkil 8.1-də göstərilmişdir. Aydındır ki, informasiya təhlükəsizliyində təhdidlərin təsnifat meyarları onların mənşəyinə və

40

www.cert.az/ziyankar.html
www.dtx.gov.az/haqqimizda1.php
www.dtx.gov.az/tarix3.php 21.
www.ict.az
https://www.javatpoint.com/cyber-security-tutorial
https://www.cybrary.it/
OWASP (Açıq Web Təhlükəsizliyi Mərkəzi) - https://owasp.org/
SANS Institute - https://www.sans.org/
Infosec Institute - https://www.infosecinstitute.com/

mənbəyinə əsaslanır. Daxili təhdidlər, adətən, öz işçilərinin və ya sistemlərinin hərəkətləri və ya hərəkətsizliyi səbəbindən təşkilat daxilindən yaranır. Bunlara qəsdən edilən hərəkətlər, məsələn, pis niyyətli işçilərin zərərli hərəkətləri, habelə nəzarətdən, səhvlərdən və ya ehtiyatsızlıqdan yaranan qəsdən olmayan hərəkətlər daxil ola bilər.



Şəkil 8.1. Təhdidlərin növləri

Müvafiq olaraq, xarici təhdidlər kənardan gələn təhlükələrdir: onlar müasir kibercinayətkarlar tərəfindən istifadə olunan metodlar toplusunu təmsil edirlər. Şəkil 8.1-dən göründüyü kimi ən məhşur xarici təhdidlərə aşağıdakılar daxildir.

DDoS hücumları[41]. Həddindən artıq yüklənməyə səbəb olmaq və işi dayandırmaq məqsədi ilə eyni vaxtda məlumat paketlərinin serverə və ya serverlər qrupuna göndərilməsini nəzərdə tutur.

41

HackRead - https://www.hackread.com/
Dark Reading - https://www.darkreading.com/
KrebsOnSecurity - https://krebsonsecurity.com/
Threatpost - https://threatpost.com/
SecurityWeek - https://www.securityweek.com/

Viruslar və casus proqramlar. Rəqəmsal texnologiyaların həyatın bütün sahələrinə nüfuz etdiyi müasir dünyada informasiya təhlükəsizliyi məsələləri getdikcə aktuallaşır. İnternet istifadəçiləri üçün əsas təhlükələrdən biri həm fərdlərə, həm də təşkilatlara ciddi ziyan vura bilən viruslar və casus proqramlar olaraq qalır.

Viruslar kompüterdəki məlumatları məhv etmək, zədələmək və ya dəyişdirmək üçün nəzərdə tutulmuş zərərli proqramlardır. Onlar yoluxmuş fayllar, e-poçtlar və ya veb saytlar kimi müxtəlif kanallar vasitəsilə yayıla bilər. Bəzi viruslar sistemlərin geniş şəkildə məhv edilməsinə səbəb olmaq, onların sıradan çıxmasına səbəb olmaq, digərləri isə məlumatı oğurlamaq və ya korlamaq üçün nəzərdə tutulub. Ən məşhur nümunələrdən biri istifadəçi fidyə ödəyənə qədər məlumatlara girişi bloklayan şifrələmə viruslarıdır.

Digər tərəfdən, casus proqramlar istifadəçi və onun onlayn fəaliyyəti haqqında gizli məlumat toplayan proqramlardır. O, şübhəli saytlar, saxta proqram yeniləmələri, hətta saxta antivirus proqramları vasitəsilə istifadəçinin xəbəri olmadan kompüterə quraşdırıla bilər. Casus proqram parolları, kredit kartı məlumatlarını və digər həssas məlumatları izləyə bilər və bu, onlayn maliyyə əməliyyatları həyata keçirən istifadəçilər üçün xüsusilə təhlükəlidir.

Viruslara və casus proqramlara qarşı mübarizənin mühüm aspektlərindən biri antivirus proqramlarının olması və əməliyyat sistemlərinin vaxtında yenilənməsidir. Bununla belə, istifadəçilər də diqqətli olmalı və potensial risklərdən xəbərdar olmalıdırlar. Məsələn, etibarsız mənbələrdən faylları yükləmək, şübhəli e-poçtları açmaq və ya şübhəli saytları ziyarət etməkdən çəkinmək vacibdir. Güclü parollardan istifadə etməyə və mümkün olduqda iki faktorlu autentifikasiyanı işə salmağa dəyər.

Təhlükəsizlik tədbirlərinin davamlı inkişafına baxmayaraq, hakerlər sistemlərə sızmaq üçün yeni üsullar icad etməyə davam edirlər. Buna görə də məlumatların təhlükəsizliyi məsələsi təkcə texniki məsələ deyil, həm də rəqəmsal gigiyena mədəniyyəti məsələsinə çevrilir. İstifadəçilərin təhlükəsizliyin əsasları üzrə maarifləndirilməsi və təşkilati səviyyədə hərtərəfli həllərin həyata keçirilməsi viruslardan və casus proqramlardan qorunmaq üçün əsas addımlardır.

Nəhayət, kibertəhlükələrin getdikcə təkmilləşdiyi bir dünyada məlumatların və məxfiliyin qorunması hər bir internet istifadəçisi üçün prioritet olmalıdır.

Məxfilik, tamlığa və əlçatanlılığa yönəlmiş təhdidlər. Şəbəkə mühəndisi təhlükəsizlik üzrə məsləhət xidmətləri təklif etməzdən əvvəl şəbəkə

infrastrukturuna real təhlükələri (məsələn, risklərin qiymətləndirilməsi və ya biznes təsirinin təhlili) başa düşməlidir. Məxfilik, bütövlük və əlçatanlıq üçün müxtəlif təhdid kateqoriyalarını aşağıdakı kimi qruplaşdırmaq olar:

- Xidmətdən imtina (DoS) və Paylanmış Xidmətdən imtina (DDoS) hücumları (Denial of Service - DoS) və Distributed Denial of Service -DDoS) hücumları.
- Spoofing (maskarad).
- Telnet hücumları.
- Şifrə sındıran proqramlar.
- Viruslar.
- Trojanlar və qurdlar.

Bu təhdidlər təsir etdikləri şəbəkə sahələri kontekstində və hədəf aldıqları dəqiq sistem komponenti nəzərə alınmaqla təhlil edilməlidir.

Xidmət hücumlarının rədd edilməsi. Xidmətdən imtina (DoS) hücumunun əsas məqsədi maşın və ya şəbəkə resursunu nəzərdə tutulan istifadəçilər üçün əlçatmaz etməkdir. Bu xüsusi hücum növündə təcavüzkar resursa giriş əldə etməyə çalışmır; daha doğrusu, o, müxtəlif istifadəçilərə və ya xidmətlərə girişin itirilməsinə səbəb olmağa çalışır. Resurslara aşağıdakılar daxil ola bilər:

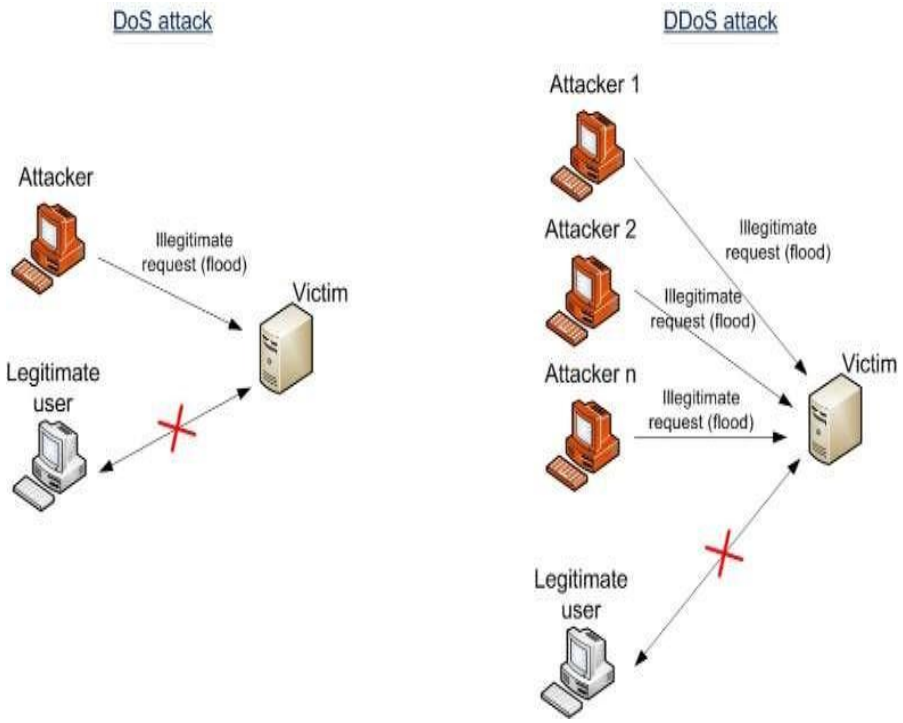
- Müəssisənin şəbəkəsi.
- Şəbəkə cihazının və ya serverinin prosessoru (CPU).
- Şəbəkə cihazının və ya serverin yaddaşı.
- Şəbəkə cihazının və ya serverin diski.

DoS hücumu resursun həddən artıq yüklənməsi ilə nəticələnir (məsələn, disk sahəsi, ötürmə qabiliyyəti, yaddaş, bufer daşması və ya növbənin daşması baxımından) və bu, resursun istifadə üçün əlçatmaz olmasına səbəb olacaq. Bu, müəyyən resursa girişin bloklanmasından tutmuş şəbəkə cihazının və ya serverin qəzaya uğramasına qədər dəyişə bilər. ICMP hücumları və TCP daşqınları kimi DoS hücumlarının bir çox növləri var. DoS hücumunun qabaqcıl forması, İnternet və ya korporativ şəbəkəsi üzərindən hədəfə hücum etmək üçün çoxlu sayda sistemləri manipulyasiya etməklə işləyən Paylanmış Xidmətdən imtinadır (DDoS). DDoS hücumunu yerləşdirmək üçün hakerlər adətən zəif qorunan hostlara daxil olurlar (məsələn, əməliyyat sistemlərində və ya istifadə olunan proqramlarda ümumi təhlükəsizlik boşluqlarından istifadə etməklə) və zərərli kod quraşdıraraq sistemləri pozurlar ki, bu da təcavüzkarın qurbanların resurslarına tam giriş imkanı verir. Bir çox sistemlər təhlükə altına düşdükdən sonra, onlar çox sayda qeyri-qanuni istəklər tərəfindən boğulacaq

hədəfə eyni vaxtda kütləvi hücum etmək üçün istifadə edilə bilər. Şəkil 8.2-də DoS hücumu ilə DDoS hücumu arasındakı fərqi göstərir.

Qeyd: Təcavüzkar tərəfindən şəbəkə resursuna qeyri-qanuni sorğuların göndərilməsi prosesi də daşqın adlanır.

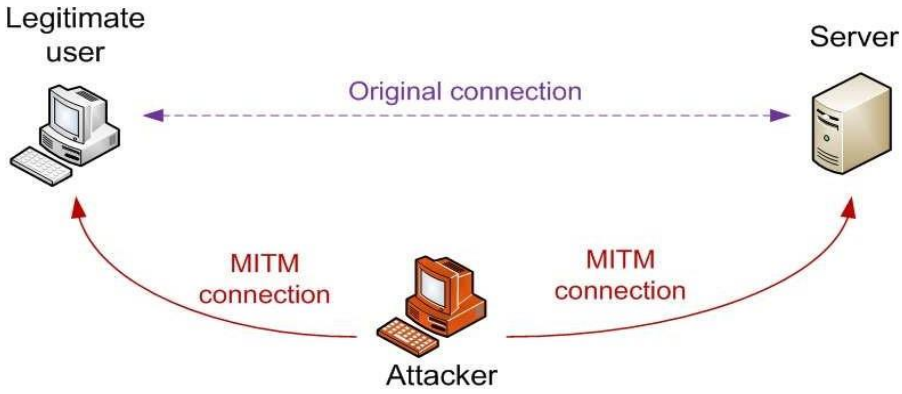
Spoofing və Man-in-the-Middle hücumları. Spoofing (və ya maskaradlama) hücumu, tək bir hostun və ya obyektin başqa bir hostun şəxsiyyətini yanlış olaraq qəbul etməsi (spoof) prosesidir. Ümumi saxtakarlıq hücumu ortada adam (MITM) hücumu adlanır və o, iki fərqli hostu (göndərən və qəbul edən) ortadakı kompüterin əslində digər host olduğuna inandırmaqla işləyir. Bu, hakerin DNS serverini pozduğu və ad həlli qeydlərini açıq şəkildə dəyişdirdiyi DNS saxtakarlığından istifadə etməklə həyata keçirilir.



Şəkil 8.2. DoS və DDoS hücumu arasındakı fərq

Başqa bir maskarad hücum növü ARP saxtakarlığıdır, burada ARP önbelleği dəyişdirilir və beləliklə, təcavüzkarın maşını vasitəsilə trafiki yönləndirmək üçün Səviyyə 2→Səviyyə 3 ünvan xəritələşdirmə qeydləri

dəyişdirilir. Bu tip hücumlar adətən Lokal Şəbəkə daxilində hədəflənir (şəkil 8.3).



Şəkil 8.3. Ortada Adam Hücumu

Telnet hücumları. Telnet və FTP kimi proqramlar istifadəçi əsaslı autentifikasiyadan istifadə edir, lakin etimadnamələr tel üzərindən aydın mətnlə (şifrlənməmiş) göndərilir. Bu etimadnamələr şəbəkə monitorinq alətlərindən istifadə edərək təcavüzkarlar tərəfindən tutula bilər və onlar şəbəkə cihazlarına icazəsiz giriş əldə etmək üçün istifadə edilə bilər. Bu sahədə digər əlaqəli təhlükələr müxtəlif sistemlərə daxil olmağa imkan verən rlogin, rcp və ya rsh kimi köhnə qorunmayan protokollardan istifadə etməklə yaradılır. Bu təminatsız protokollar SSH və ya SFTP kimi protokollarla əvəz edilməlidir.

Parolun sınması. Parolun sındırılması üçün proqram təminatı bu gün tapmaq çox asandır və o, müxtəlif tətbiqlərdə və ya xidmətlərdə parol təhlükəsizliyini pozmaq üçün istifadə edilə bilər. Proqram təminatı əvvəllər zəif şifrələmə alqoritmləri (məsələn, DES) ilə şifrələnmiş parolu aşkar etməklə işləyir. Parolun sınmasının qarşısını almağın bir yolu şirkətin təhlükəsizlik siyasətini tətbiq etməkdir:

- Güclü şifrələmə alqoritmlərindən istifadə (məsələn, AES).
- Mürəkkəb parolların seçilməsi (hərflərin, rəqəmlərin və xüsusi simvolların birləşməsi).
- Parolların vaxtaşırı dəyişdirilməsi.

Viruslar. Virus hədəf sistemdə fərdi fayllara qoşulan hər hansı bir proqram növü üçün ümumi termindir. Virus orijinal kodunu qurbanın faylına əlavə etdikdən sonra qurban yoluxmuş olur və fayl dəyişdirilir və replikasiya adlanan proses vasitəsilə digər faylları yoluxa bilər. Replikasiya prosesi sabit

disklərə yayıla bilər və bütün əməliyyat sistemini yoluxdura bilər. Bir virus icra edilə bilən faylla əlaqələndirildikdən sonra, host faylı hər dəfə icra edildikdə digər faylları yoluxduracaq. Etdikləri yerdən asılı olaraq üç əsas virus növü var:

- MBR (Master Boot Sector) virusları.
- Yükləmə sektoru virusları.
- Fayl virusları.

MBR və yükləmə sektoru virusları fiziki diskdəki yükləmə sektoruna təsir edir və əməliyyat sistemini yükləyə bilmir. Fayl virusları ən çox yayılmış virus növünü təmsil edir və müxtəlif növ faylları təsir edir.

Virusları təsnif etməyin başqa bir yolu onların davranışlarına əsaslanır, bunların iki növü var:

1. Gizli viruslar.
2. Polimorf viruslar.

Gizli viruslar disk sürücüsündə dəyişiklik edildiyini gizlətmək üçün müxtəlif üsullardan istifadə edir. Polimorf virusları müəyyən etmək çətindir, çünki onlar mutasiya edə bilirlər, yəni ölçülərini dəyişə bilirlər və virus skanerləri tərəfindən aşkarlanmaqdan qaça bilərlər. Bu virus aşkarlama proqramlarından istifadə edərkən tövsiyə olunur ki, onların mümkün qədər tez-tez yenilənməsinə əmin olun ki, virusların yeni formalarını skan edə bilsinlər.

Trojanlar və qurdlar. Trojan proqramları əsasən qanuni proqramlarda olan və istifadəçi üçün gizli olan funksiyaları yerinə yetirən icazəsiz kodlardır. Qurdlar e-poçtlara əlavə oluna bilən digər qeyri-qanuni proqram təminatı parçalarıdır və onlar icra edildikdən sonra fayl sistemi daxilində yayıla və istifadəçi trafikini müəyyən veb-saytlara yönləndirmə kimi icazəsiz funksiyaları yerinə yetirə bilərlər.

Sosial mühəndislik hücumları. İnternet istifadəçilərinin sayının artması və müxtəlif onlayn platformaların çoxalması ilə sosial mühəndislik hücumları inkişaf etməyə davam edir, daha mürəkkəb və geniş yayılır. Bu hücumlar ölçüsündən və təhlükəsizlik səviyyəsindən asılı olmayaraq həm şəxslər, həm də təşkilatlar üçün təhlükə yaradır. Sosial mühəndislik, məxfi məlumatları əldə etmək, sistemlərə daxil olmaq və ya təcavüzkarın maraqları naminə müəyyən hərəkətlər etmək üçün insanlara psixoloji təsirə əsaslanan kiberhücum metodudur. Proqram təminatı və ya şəbəkələri sındırmağa yönəlmiş ənənəvi haker hücumlarından fərqli olaraq, sosial mühəndislik insanları, onların davranışlarını və psixoloji xüsusiyyətlərini hədəf alır. Sosial mühəndislik hücumçuları qurbanlarının inandırıcılığını, qorxularını və ya maraqlarını

manipulyasiya edirlər. Nəticədə, qurbanlar könüllü olaraq şəxsi məlumatlara, parollara, maliyyə məlumatlarına və ya digər qiymətli resurslara onların hədəf alındığını fərq etmədən çıxışı təmin edə bilərlər.

Sosial mühəndisliyin mahiyyəti insanı aldadaraq, təcavüzkar üçün faydalı olan müəyyən hərəkətləri yerinə yetirməkdən ibarətdir. Sosial mühəndislik üsulları istifadəçilərə şəxsi məlumat tələb edən saxta mesajların göndərildiyi fişinqdən tutmuş vishing (səsli fişinq) və pharming (saxta veb saytlara yönləndirmə) kimi müxtəlif ola bilər. Sosial mühəndislik hücumunun əsas məqsədi manipulyasiya və aldatma yolu ilə qorunan məlumat və ya resurslara çıxış əldə etməkdir. Şirkət işçiləri tez-tez bu cür hücumların hədəfinə çevrilirlər, çünki onlar korporativ sistemlərə və məlumatlara girişi təmin edə bilirlər və bundan sonra növbəti hücumlar və ya qəsb üçün istifadə edilə bilər.

Sosial mühəndislik, qurbanın tez və düşünmədən hərəkət etməsinə səbəb olan yanlış təcililik hissi yaratmaq üçün də istifadə edilə bilər. Məsələn, təcavüzkar özünü texniki dəstək işçisi kimi göstərə və istifadəçidən sistemə giriş imkanı verərək təcili olaraq şifrəni dəyişməsini istəyə bilər.

Beləliklə, sosial mühəndislik hücumları əhəmiyyətli təhlükə yaradır, çünki onlar texniki zəifliklərdən çox insan emosiyalarının və davranışlarının manipulyasiyasına əsaslanır. İstifadəçilərin bu hücumlara qarşı necə mübarizə aparacağına dair məlumatlılıq və təlim sosial mühəndislikdən qorunmaqda mühüm addımdır.

Sosial mühəndislik hücumlarını istifadə edilən üsullardan və hücumçuların məqsədlərindən asılı olaraq bir neçə əsas növə bölmək olar: Fişinq, Smişinq, Vişing, Pretekstinq, Beytinq, Farminq, Təqlidetmə,Tailgating, İkiqat spirinq və s. Bu cür hücumların təsnifatı onların mahiyyətini daha yaxşı anlamağa və onlardan qorunmaq üçün strategiyalar hazırlamağa kömək edir.

Fişinq sosial mühəndisliyin ən geniş yayılmış formalarından biridir, bu zaman təcavüzkarlar saxta e-poçtlar, mesajlar göndərir və ya saxta veb-saytlar yaradaraq istifadəçiləri parollar, kredit kartı məlumatları və girişlər kimi həssas məlumatlarla təmin edirlər. Nümunə olaraq, Hesab məlumatlarınızı yeniləməyinizi xahiş edən banklardan gəldiyini iddia edən mesajlar, şəxsi məlumatların təsdiqini tələb edən "dəstək xidmətlərindən" məktublar və s. göstərmək olar.

Smişinq hücumun SMS mesajları vasitəsilə baş verdiyi bir fişinq növüdür. Təcavüzkarlar saxta saytlara keçidlər olan mesajlar göndərirlər və ya istifadəçini şəxsi məlumatlarını təhvil verməyə təşviq edirlər. Nümunə olaraq, Əməliyyatın təsdiqlənməsi və ya məlumatların yenilənməsi tələbi ilə "bankdan"

SMS, "Çatdırılma xidmətlərindən" mesajlar bağlamanızı izləmək üçün linkə daxil olmanızı xahiş edir. və s. göstərmək olar.

Vişinq telefon zənglərindən istifadə edilən hücumdur. Təcavüzkarlar qurbanı məxfi məlumatları təhvil verməyə və ya müəyyən hərəkətlər etməyə inandırmaq üçün özlərini şirkətlərin, bankların və ya dövlət qurumlarının işçiləri kimi göstərə bilərlər. Nümunə olaraq, "Yoxlama" üçün kart təfərrüatlarını tələb edən "bank işçisindən" zəng, Məlumat təqdim edilmədiyi təqdirdə sanksiyalarla hədələyən “vergi xidmətindən” zəng və s. göstərmək olar.

Pretekstinq təcavüzkarın qurbanın etibarını qazanmaq və məlumat və ya resurslara çıxış əldə etmək üçün saxta ssenari və ya örtük hekayəsi yaratdığı bir texnikadır. Burada əsas diqqət inandırıcı hekayə yaratmaqdır. Nümunə olaraq, şifrələri əldə etmək üçün özünü şirkətin İT xidmətinin əməkdaşı kimi göstərmək, yanlış vəziyyət yaratmaq, məsələn, "təhlükəsizlik yoxlamaları üçün" şəxsi məlumatların tələb edilməsi və s. göstərmək olar.

Beytinq qurbanı cəlb etmək və onu təcavüzkarın maraqlarına uyğun hərəkət etməyə məcbur etmək üçün cazibələrdən istifadə etməyi əhatə edir. Bu, yoluxmuş USB sürücüsü kimi fiziki cazibə və ya cazibədar təklif şəklində rəqəmsal cazibə ola bilər. Nümunə olaraq, görünən yerdə qalan və zərərli proqram ehtiva edən “Məxfi” qeyd edilmiş USB sürücüsü, Viruslarla yoluxmuş məşhur proqram təminatının pulsuz yüklənməsi üçün saxta təkliflər və s. göstərmək olar.

Farminq düzgün URL daxil olsa belə, istifadəçilərin saxta veb-saytlara yönləndirildiyi bir hücumdur. Bu hücum istifadəçinin kompüterini zərərli proqramla yoluxdurmaqla və ya DNS serverini sındırmaqla həyata keçirilə bilər. Nümunə olaraq, düzgün ünvanı daxil etmələrinə baxmayaraq istifadəçilərin yönləndirildiyi saxta bank saytları, saxta onlayn mağazalar real mağazalar kimi maskalanır və s. göstərmək olar.

Təqlid təcavüzkarın resurslara və ya məlumatlara çıxış əldə etmək üçün başqa bir şəxs kimi göründüyü hücumdur. Bu, real insan (məsələn, həmkar, patron) və ya uydurma bir fiqur (məsələn, yardım masasının əməkdaşı) ola bilər. Nümunə olaraq, özünüzü müdir kimi təqdim edin və təcili pul köçürməyinizi xahiş edin, korporativ məlumatlara giriş əldə etmək üçün həmkarını təqlid etmək və s. göstərmək olar.

Tailqeytinq təcavüzkarın qanuni girişi olan birini izləyərək qorunan əraziyə daxil olduğu sosial mühəndisliyin fiziki formasıdır. Bu üsul xüsusilə ofislərdə və nişan sistemi olan digər yerlərdə geniş yayılmışdır. Nümunə olaraq,

girişi olan bir işçini izləyərək ofis binasına daxil olmaq, insanların sadəlövhlüyündən istifadə edərək sənədləri yoxlamadan qorunan əraziyə daxil olmaq və s. göstərmək olar.

Snappinq bir şəxsin parol və ya PİN kodu daxil etməsinə baxmaq kimi cihazlara və ya resurslara giriş əldə etmək üçün sosial mühəndislikdən istifadəni nəzərdə tutur. Nümunə olaraq, Bir şəxsin bankomata giriş kodunu daxil etməsinə baxmaq, Bir işçinin iş kompüterinə parol daxil etməsinə nəzarət.

İkiqat spirinq təcavüzkarların əvvəlcə daha az qorunan hədəflərə hücum etdiyi və sonra əldə edilən məlumatlardan əsas hədəfə hücum etmək üçün istifadə etdiyi hədəflənmiş hücumdur. Nümunə olaraq, menecerin korporativ elektron poçtuna daxil olmaq üçün tabeçiliyə hücum, Sonrakı, daha böyük hücumlar üçün pozulmuş məlumatlardan istifadə və s. göstərmək olar.

Sosial mühəndislik hücumları müxtəlif formalarda ola bilər, lakin onların hamısı təcavüzkarların məqsədlərinə çatmaq üçün insan amillərindən istifadə etmək məqsədi daşıyır. Bu hücumların təsnifatını başa düşmək onlara daha yaxşı hazırlaşmağınıza və istifadəçilərin təlimi və autentifikasiyanın əlavə təbəqələrinin həyata keçirilməsi də daxil olmaqla effektiv müdafiə vasitələrini inkişaf etdirməyə kömək edir.

Bufer daşması hücumları. Bufer daşması hücumu tətbiqin zəifliyindən istifadə edən hücumdur. Tətbiqlərin yaddaşında bufer adlanan müxtəlif saxlama sahələri var və siz bufer ölçüsündən daha çox məlumat saxlamağa cəhd etsəniz, məlumatlar əldə edilməməsi lazım olan qonşu yaddaş sahələrinə "tökülə bilər". Təcavüzkar bu davranışdan istifadə edə bilər və bunun icrası üçün müəyyən yaddaş sahələrində zərərli proqram kodu yaza bilər. Təcavüzkar mümkün bufer daşmasını aşkar etdikdən sonra, bu o demək deyil ki, o, bunu zəiflik hesab edə bilər. Diqqətli təhlil aparılmalıdır, çünki buferin bir çox dəfə daşması proqramın sadəcə çökməsinə səbəb ola bilər. Bufer daşması zəifliyindən istifadə etmək qərarına gələn təcavüzkar, nə qədər və hansı növ məlumatların yeridilməsi lazım olduğunu dəqiq müəyyənləşdirməlidir. Bufer daşması təkrarlanan və proqnozlaşdırıla bilən şəkildə həyata keçirilə bilərsə, təcavüzkar sistemi ələ keçirə bilər. Tərtibatçıların lazımi yoxlamalar aparması və məlumatların nə və harada daxil edilməsinə məhdudiyyətlər qoyması ilə bufer daşması hücumlarının qarşısı alına bilər. Tərtibatçılar üçün sınaq üçün ciddi vaxt ayırmaq çox vacibdir, çünki mümkün təcavüzkarların da tətbiqlərdə zəif cəhətləri axtarmaq üçün çox vaxtı var. Bufer daşqın hücumlarından qorunmağın başqa bir yolu müntəzəm sistem yamaları yerinə yetirməkdir, çünki müntəzəm olaraq yeni zəifliklər aşkar edilir.

Wİ-Fİ ZƏİFLİKLƏRİ

Simsiz şəbəkələr[42] açıq strukturlarına görə simli şəbəkələrə nisbətən hücumlara qarşı daha həssas ola bilər, çünki potensial təcavüzkarlar müəssisənin binalarına faktiki giriş əldə etmədən şəbəkəni poza bilər. Wi-Fi şəbəkələri, onların rahatlığına və geniş istifadəsinə baxmayaraq, onları müxtəlif təhlükələrə qarşı həssas edən bir sıra zəif cəhətlərə malikdir. Əsas problemlərdən biri məhdud təhlükəsizlikdir. Bir çox şəbəkələr WEP və ya WPA kimi köhnəlmiş şifrələmə protokollarından istifadə edir, onları qırmaq asandır. Zəif parollar və ya standart marşrutlaşdırıcı parametrləri istifadə edildikdə, hətta WPA2 ilə müasir şəbəkələr də həssas ola bilər. Əlavə təhlükə hər kəsin qoşula biləcəyi, heç bir məhdudiyyət olmadan məlumat və resurslara çıxış əldə edən qorunmayan şəbəkələrdir. Wi-Fi-ın digər zəif cəhəti onun məhdud əhatə dairəsi və ölü zonaların olmasıdır. Böyük binalarda və ya evlərdə divarlar və mebel kimi fiziki maneələr səbəbindən bəzi yerlərdə siqnal zəif və ya tamamilə olmaya bilər. Digər elektron cihazların müdaxiləsi də siqnal keyfiyyətini aşağı sala bilər, xüsusən də insanların sıx olduğu yerlərdə və ya çoxlu yaxınlıqda şəbəkələri olan evlərdə. Bu, zəif performansa, daha yavaş məlumat ötürmə sürətlərinə və qeyri-sabit bağlantılara gətirib çıxarır. Zəif şəbəkə performansı çox vaxt sıxlıqla əlaqələndirilir: çoxlu sayda qoşulmuş qurğular Wi-Fi işini əhəmiyyətli dərəcədə ləngidə bilər. Bu, maksimum məlumat ötürmə sürətini məhdudlaşdıran köhnə standartlardan istifadə edən şəbəkələr üçün xüsusilə doğrudur. Qeyri-kafi buraxma qabiliyyəti və digər şəbəkələrin müdaxiləsi də əlaqə keyfiyyətinin pisləşməsində böyük rol oynayır. Hücumlara qarşı zəiflik Wi-Fi şəbəkələrinin digər əsas problemidir. Saxta giriş nöqtələrindən istifadə kimi sosial mühəndislik hücumları istifadəçiləri təhlükəli şəbəkələrə qoşulmaq üçün asanlıqla aldada bilər. Müvafiq monitorinq və giriş nəzarəti olmadan, icazəsiz giriş və sui-istifadə riskini artıraraq, şəbəkəyə hansı cihazların qoşulduğunu və nə etdiklərini izləmək çətindir.

Wi-Fi zəifliklərini müəyyən etmək üçün aşağıdakı yanaşmalardan istifadə edilə bilər:

42

Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.

Зима В.М. Безопасность глобальных сетевых технологий / В.М.Зима, А.А.Молдовян, Н.А.Молдовян. СПб.; БХВ-Петербург, 2019. – 320 с

- Təhlükəsizlik parametrlərinin təhlili.
- Şəbəkənin əhatə dairəsi və performans auditi.
- Performans testi.
- Giriş nəzarəti reytinqi.
- Xüsusi alətlərdən istifadə edərək zəifliyin təhlili.
- Nəzarət və monitorinq yoxlaması.

Təhlükəsizlik parametrlərinin təhlili istifadə olunan şifrələmənin və parolların keyfiyyətinin yoxlanılmasını əhatə edən əsas addımdır. Müasir şəbəkələr güclü parollarla WPA3 və ya minimum WPA2-dən istifadə etməlidir. Router parametrlərinin təhlükəsiz olduğundan əmin olmaq da vacibdir, məsələn, administrator parolu dəyişdirilir və proqram təminatı yenilənir.

Şəbəkənin əhatə dairəsi və performansının auditi siqnal gücünü və ölü zonaların mövcudluğunu qiymətləndirməyə imkan verir. Wi-Fi analizatorlarından istifadə edərək binanın müxtəlif hissələrində siqnal gücünü ölçə və əhatə dairəsi az olan və ya olmayan sahələri müəyyən edə bilərsiniz. Bu proses həmçinin digər simsiz şəbəkələr və ya elektron cihazlar kimi əlaqənizi alçaldan müdaxiləni müəyyən etməyə kömək edir.

Performans testi əlaqənin sürətini və sabitliyini qiymətləndirmək məqsədi daşıyır. Şəbəkənin müxtəlif nöqtələrində bu testləri həyata keçirməklə, təkmilləşdirilməsi lazım olan şəbəkə zəifliklərini göstərən aşağı məlumat sürəti və yüksək gecikmə olan sahələri müəyyən etmək mümkündür. Bu, şəbəkə sıxlığı və ya köhnəlmiş Wi-Fi standartları ilə bağlı problemlərin aradan qaldırılması üçün xüsusilə vacibdir.

Girişə nəzarət reytinqi əlaqənin idarə edilməsinə diqqət yetirir. Buraya hansı cihazların şəbəkəyə daxil olduğunu və onların autentifikasiyasını yoxlamaq daxildir. Giriş nəzarətinin zəif tərəflərinin müəyyən edilməsi icazəsiz qoşulma riskini minimuma endirməyə və şəbəkə təhlükəsizliyini yaxşılaşdırmağa kömək edə bilər.

Xüsusi alətlərdən istifadə edərək zəifliyin təhlili potensial təhlükələri daha dərindən araşdırmaq imkanı verir. Wireshark kimi alətlər şəbəkə trafikini təhlil edə və adam-in-the-middle kimi mümkün hücumları müəyyən edə bilər. Tədqiqatçılar həmçinin şəbəkəyə müdaxilənin və məlumatlara çıxış əldə etməyin nə qədər asan olduğunu müəyyən etmək üçün penetrasiya testi vasitələrindən istifadə edə bilərlər.

Nəzarət və monitorinq yoxlamasına şəbəkə fəaliyyətinin müntəzəm monitorinqi və şübhəli fəaliyyətlər haqqında xəbərdarlıq daxildir. Bu, potensial təhlükələrə və şəbəkədəki dəyişikliklərə tez reaksiya verməyə imkan verir.

Monitorinq sistemlərinin mövcudluğu icazəsiz giriş cəhdlərini vaxtında aşkar etməyə və Wi-Fi şəbəkəsinin ümumi təhlükəsizliyini yaxşılaşdırmağa kömək edir.Wi-Fi zəifliklərinin müəyyən edilməsi və onların aradan qaldırılması təhlükəsiz və etibarlı şəbəkənin təmin edilməsində mühüm addımdır. Müasir alətlər və texnologiyalardan istifadə riskləri minimuma endirməyə və məlumatları potensial təhlükələrdən qorumağa kömək edəcək. Şəbəkə konfiqurasiyanızı müntəzəm olaraq yoxlamaq və yeniləmək təhlükəsiz mühiti qorumaq üçün zəruri təcrübədir.

ŞƏBƏKƏ CİHAZI ZƏİFLİKLƏRİ

Yuxarıda göstərilən hücumları nəzərə alsaq, şəbəkə infrastrukturunda mühüm həssas sahə şəbəkə qurğularından ibarətdir. Marşrutlaşdırıcılar, açarlar, şəbəkə adapterləri və s. kimi şəbəkə qurğularının bir sıra zəif cəhətləri var ki, bu da təcavüzkarlar tərəfindən şəbəkə təhlükəsizliyinə hücum etmək və pozmaq üçün istifadə edilə bilər. Şəbəkə cihazı zəifliklərinə aşağıdakılar daxildir:

- Proqram təminatının zəifliklər.
- Konfiqurasiyanın zəif tərəfləri.
- Xidmətdən imtina (DDoS) hücumları.
- Fiziki zəifliklər.
- Protokol təhlükəsizliyi problemləri.
- Şifrələmənin olmaması.
- Proqram təminatı yeniləmələrinin olmaması.

Proqram təminatı zəifliklər çox vaxt koddakı səhvlərdən və ya sistem arxitekturasındakı qüsurlardan yaranır. Bu boşluqlar təcavüzkarlara ixtiyari kod icra etməyə, icazəsiz giriş əldə etməyə və ya cihazın işini pozmağa imkan verə bilər. Məlum zəifliklər bağlamaq üçün şəbəkə cihazlarının proqram təminatını və proqram təminatını mütəmadi olaraq yeniləmək vacibdir.

Konfiqurasiya zəifliklər başqa bir ümumi problemdir. Yanlış təhlükəsizlik parametrləri, standart parolların istifadəsi, şəbəkə seqmentasiyasının olmaması və ya yanlış konfiqurasiya edilmiş giriş siyasəti hücumlara qapı aça bilər. Diqqətsiz və ya qeyri-kafi konfiqurasiya səbəbindən şəbəkələr tez-tez həssas qalır.

Xidmətdən imtina (DDoS) hücumları şəbəkə cihazlarını istəklərlə sıxışdıraraq və qanuni istifadəçilər üçün əlçatmaz etməklə onlara təhlükə

yaradır. Cihazlar böyük həcmdə trafiki idarə edə bilmirsə, bu, şəbəkənin əhəmiyyətli dərəcədə pozulmasına səbəb ola bilər.

Fiziki zəifliklər də şəbəkə cihazlarının təhlükəsizliyində mühüm rol oynayır. Cihazlara fiziki giriş təcavüzkarlara onları manipulyasiya etməyə, söndürməyə və ya dəyişdirməyə imkan verir ki, bu da məlumat sızmasına və ya şəbəkənin pozulmasına səbəb ola bilər. Xüsusilə ictimai və ya kilidi açıq ərazilərdə cihazlar üçün güclü fiziki təhlükəsizlik vacibdir.

Köhnəlmiş və ya etibarlı olmayan rabitə protokollarından istifadə edildikdə protokol təhlükəsizliyi problemləri yaranır. Məsələn, məlumat ötürülməsi üçün təhlükəli protokolların istifadəsi təcavüzkarlara trafikin qarşısını almağa və ya dəyişdirməyə imkan verə bilər. Bu cür riskləri azaltmaq üçün güclü şifrələmə və autentifikasiyaya malik müasir protokollar tətbiq edilməlidir.

Şəbəkə cihazları üzərindən ötürülən məlumatların şifrələnməməsi ciddi təhlükəsizlik riski yaradır. Şifrələnməmiş məlumatlar təcavüzkarlar tərəfindən asanlıqla tutula və istifadə edilə bilər. Bu, icazəsiz girişdən qorunma tələb edən məxfi məlumatlar üçün xüsusilə vacibdir.

Proqram təminatının yenilənməsinin olmaması şəbəkə qurğusunun zəifliyinin əsas səbəblərindən biridir. İstehsalçılar aşkar edilmiş zəiflikləri aradan qaldırmaq və təhlükəsizliyi artırmaq üçün müntəzəm olaraq yeniləmələr buraxırlar. Bu yeniləmələr vaxtında quraşdırılmasa, qurğular hücumlara qarşı həssas olaraq qalır.

Bu zəifliklərin hər biri etibarlı şəbəkə qorunmasını təmin etmək və hücum riskini minimuma endirmək üçün diqqət və azaldıcı tədbirlər tələb edir.

TƏHLÜKƏSİZLİK TƏHDİDLƏRİ VƏ RİSKLƏRİ

Şəbəkə təhlükəsizliyi təhdidləri və riskləri müasir informasiya sistemlərində mühüm aspektlərdəndir, çünki kiberhücumların sayının və mürəkkəbliyinin artması şəbəkə infrastrukturunun qorunması ehtiyacını artırır. Bu məsələyə giriş ondan ibarətdir ki, şəbəkələr həm biznesdə, həm də gündəlik həyatda işlərin necə işlədiyinin mərkəzinə çevrilir. Onlar məlumat mübadiləsini, resurslara çıxışı və cihazlar arasında qarşılıqlı əlaqəni təmin edir. Bununla belə, şəbəkələrdən istifadə artdıqca məlumatın məxfiliyinə, bütövlüyünə və əlçatanlığına təsir göstərə biləcək təhlükələrin sayı da artır.

Şəbəkə təhlükəsizliyi məsələsinin aktuallığı onunla bağlıdır ki, şəbəkələrə uğurlu hücumlar təşkilatlar və fərdi istifadəçilər üçün fəlakətli nəticələr verə bilər. Məlumat itkisi, xidmətin pozulması və maliyyə itkisi nəticələrdən yalnız bir neçəsidir.

Rəqəmsal transformasiya dövründə, getdikcə daha çox proses və xidmətlərin onlayn rejimdə hərəkət etdiyi bir vaxtda şəbəkə təhlükəsizliyinin təmin edilməsi biznes və dövlət qurumları üçün prioritet məsələyə çevrilir. Şəbəkə təhlükəsizliyi təhdidlərinin və risklərinin mahiyyəti təcavüzkarların şəbəkələrə hücum etmək üçün istifadə etdikləri üsul və yanaşmaların müxtəlifliyindədir. Bu təhdidlərə proqram hücumları, parol sındırma cəhdləri, ortada adam hücumları, fişinq hücumları, zərərli proqramların paylanması və şəbəkə cihazlarına fiziki hücumlar daxil ola bilər. Risklər uğurlu hücum ehtimalı və şəbəkə və onun istifadəçiləri üçün mümkün nəticələrlə bağlıdır. Bunun üçün zəiflikləri minimuma endirmək və şəbəkə infrastrukturunun potensial təhlükələrə davamlı olmasını təmin etmək üçün davamlı monitorinq, təhlükəsizlik yeniləmələri və işçilərin təlimi tələb olunur.

Şəbəkə təhdidləri aşağıdakı növlərə bölünə bilər:

- Kəşfiyyat.
- İcazəsiz giriş.
- Xidmətdən imtina (DoS).

Təhlükənin bir növü hədəf sistem və ya şəbəkə haqqında məlumat toplamaqdan ibarət olan kəşfiyyatdır. Təcavüzkarlar zəiflikləri müəyyən etmək üçün portların skan edilməsi, trafikin təhlili və digər üsullar kimi müxtəlif üsullardan istifadə edirlər. Kəşfiyyatın məqsədi sonrakı hücumlara hazırlaşmaq üçün şəbəkə, onun strukturu, istifadə olunan qurğular və protokollar haqqında mümkün qədər çox məlumat əldə etməkdir. Kəşfiyyat fəaliyyətləri tez-tez aşkar edilmir və onları xüsusilə təhlükəli edir, çünki onlar aktiv hücumlara başlamazdan əvvəl təcavüzkarların gizli qalmasına imkan verir.

Şəbəkə təhlükəsinin digər mühüm növü icazəsiz girişdir. Təcavüzkarlar icazəsiz şəbəkə resurslarına daxil olmaq üçün zəif parollardan, proqram təminatının zəifliklərindən və ya sosial mühəndislik hücumlarından istifadə edə bilərlər. İcazəsiz giriş təcavüzkarlara məlumatları manipulyasiya etmək, zərərli proqram quraşdırmaq və ya şəbəkədən hücumların sonrakı yayılması kimi öz məqsədləri üçün istifadə etməyə imkan verir. Bu təhlükə xüsusilə təhlükəlidir, çünki o, uzun müddət aşkarlanmadan qala bilər və təcavüzkarın şəbəkədə gizli və dağıdıcı fəaliyyətlər həyata keçirməsinə imkan verir.

Xidmətdən imtina (DoS) şəbəkə xidmətlərini pozmağa yönəlmiş şəbəkə təhlükəsinin başqa bir növüdür. DoS hücumları və ya paylanmış hücumlar (DDoS) şəbəkə və ya serveri sorğularla həddən artıq yükləmək məqsədi daşıyır, nəticədə resurslar qanuni istifadəçilər üçün əlçatmaz olur. Bu cür hücumlar təşkilatlara əhəmiyyətli ziyan vura bilər, xüsusən də onların onlayn xidmətlərinin davamlı fəaliyyətindən asılı olduqda. DoS hücumları ya hədəflənmiş, ya da şəbəkənin sabitliyini pozmağa yönəlmiş daha böyük hücumların bir hissəsi ola bilər.

Zəifliklərə kəşfiyyat hücumları, icazəsiz giriş və ya DoS hücumları kimi təhdidlərin mənfi təsir ehtimalının göstəricisi kimi baxmaq olar. Bu zəifliklər sistemləri şəbəkə infrastrukturunun təhlükəsizliyinə birbaşa təsir edən müxtəlif risklərə məruz qoya bilər. Şəbəkə təhlükəsizliyi risklərinə aşağıdakılar daxildir:

- Məlumat oğurluğu.
- Məlumatların kompromissi.
- Əlçatanlığın itirilməsi.
- İcazəsiz giriş.
- Sistem zəifliyinin artırılması.
- Maliyyə itkiləri.
- Reputasiyaya zərər.

Sistemdəki boşluqlar təcavüzkarlara həssas məlumatlara icazəsiz giriş əldə etməyə imkan verə bilər. Bura şəxsi məlumatlar, maliyyə məlumatları, korporativ sirlər və əhəmiyyətli maliyyə və nüfuz itkiləri ilə nəticələnə biləcək digər qiymətli məlumatlar daxil ola bilər. Təcavüzkar sistemə giriş əldə edərsə, məlumatları dəyişdirə, korlaya və ya silə bilər. Bu, məlumatın təhrif olunmasına, sistem xətalarına və mühüm məlumatların itirilməsinə gətirib çıxara bilər ki, bu da biznes proseslərinə və qərarların qəbuluna mənfi təsir göstərəcək. DoS və ya DDoS hücumları şəbəkə resurslarını həddən artıq yükləyə bilər və bu, onları qanuni istifadəçilər üçün əlçatmaz edir. Bu, biznes proseslərinin dayanmasına, gəlir itkisinə və müştəri xidmətinin pisləşməsinə səbəb ola bilər. Zəifliklər təcavüzkarlara girişi olmayan sistemlərə və resurslara giriş əldə etməyə imkan verə bilər. Bu, resursların icazəsiz istifadəsinə, zərərli fəaliyyətlərə və ya həssas məlumatların toplanmasına səbəb ola bilər. Sistemin bir hissəsindəki boşluqlar şəbəkənin və ya sistemin digər hissələrinə hücum etmək üçün istifadə edilə bilər. Bu, təhdidlərin daha da yayılmasına və hücumun miqyasının artmasına səbəb ola bilər. Zəifliklər və hücumların nəticələri sistemin bərpası, zərərin ödənilməsi, cərimələr və digər xərclərlə bağlı

əhəmiyyətli maliyyə itkilərinə səbəb ola bilər. Bu da şirkətin səhmlərinin qiymətinə və maliyyə sabitliyinə təsir edə bilər. İctimai təhlükəsizlik insidentləri şirkətin reputasiyasına xələl gətirərək müştərilər, tərəfdaşlar və ictimaiyyət arasında etibarın itirilməsinə səbəb ola bilər. Reputasiyanızı bərpa etmək xeyli səy və vəsait tələb edə bilər.

Beləliklə, zəifliklər operativ həll edilmədikdə müxtəlif şəbəkə təhlükəsizliyi riskləri yarana bilər.

ETİBARLILIQ VƏ KİMLİYİN İDARƏ OLUNMASI

Güvən və şəxsiyyətin idarə edilməsi[43] təhlükəsiz şəbəkə sistemlərinin inkişafında mühüm aspektdir. Güvən və şəxsiyyət idarəetməsi şəbəkəyə kimin daxil ola biləcəyini, hansı sistemlərin şəbəkəyə daxil ola biləcəyini, şəbəkəyə nə vaxt və harada daxil ola biləcəyini və girişin necə baş verə biləcəyini bildirir. O, həmçinin yoluxmuş maşınları təcrid etməyə və onların imza verilənlər bazalarını və tətbiqlərini yeniləməyə məcbur olduğu giriş nəzarətini tətbiq etməklə onları şəbəkədən kənarda saxlamağa çalışır.

Güvən və şəxsiyyət idarəetməsi üç komponentdən ibarətdir:

- Güvən.
- Şəxsiyyət.
- Giriş nəzarəti.

Güvən iki və ya daha çox şəbəkə obyekti, məsələn, iş stansiyası və təhlükəsizlik divarı cihazı arasındakı əlaqədir. Güvən konsepsiyası təhlükəsizlik siyasəti qərarlarını müəyyən edəcək. Etibar əlaqəsi varsa, qurumlar arasında ünsiyyətə icazə verilir. Etibar münasibətləri və imtiyaz səviyyəsi müxtəlif pozalardan təsirlənə bilər (məsələn, köhnəlmiş virus imza bazası və ya yamaqsız sistem). Cihazlar müxtəlif səviyyələrdə seqmentasiyaya malik ola bilən etibar domenlərinə qruplaşdırıla bilər.

Şəxsiyyət aspekti istifadəçilər, cihazlar və ya digər təşkilatlar daxil olmaqla, kimin şəbəkəyə daxil ola biləcəyini müəyyən edir. Şəxsiyyətin autentifikasiyası giriş nəzarəti ilə əlaqə yaradan üç atribut əsasında aparılır:

- Subyektin bildiyi bir şey (parol və ya PİN)

43

Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.

- Mövzunun malik olduğu bir şey (token və ya smart kart)
- Mövzunun olduğu bir şey (barmaq izi, səs və ya üz tanıma kimi biometrik məlumatlar).

Güvən domenləri Microsoft Active Directory tətbiqində və böyük təşkilatlarda və İnternetdə həyata keçirilə bilər. Sertifikatlar istifadəçi şəxsiyyətinin və məlumat və xidmətlərə daxil olmaq hüququnun təsdiqində mühüm rol oynayır.

Müəssisə təşkilatlarında giriş nəzarəti adətən AAA (Autentifikasiya, Avtorizasiya və Mühasibatlıq) xidmətlərinə əsaslanır. AAA həlləri bəzi back-end xidmətlərindən və müxtəlif RADIUS və ya TACACS+ serverlərindən istifadə edə bilən aralıq autentifikator cihazdan (məsələn, marşrutlaşdırıcı, keçid və ya firewall) istifadə edə bilər. Doğrulama istifadəçi və ya sistem şəxsiyyətini və şəbəkə resurslarına çıxışı müəyyən edir, avtorizasiya xidmətləri isə istifadəçilərin nəyə daxil ola biləcəyini müəyyənləşdirir. Mühasibat hissəsi faktura xidmətləri üçün istifadə edilə bilən audit cığırını təqdim edir (məsələn, istifadəçinin müəyyən xidmətə qoşulma müddətini qeyd etmək). Müasir şəbəkə cihazlarının əksəriyyəti autentifikator kimi çıxış edə bilər və istifadəçinin autentifikasiya sorğularını RADIUS/TACACS+ serverlərinə ötürə bilər.

Təhlükəsiz əlaqə. Təhlükəsiz əlaqə ötürülən məlumatların məxfiliyini, bütövlüyünü və autentifikasiyasını təmin edən iki və ya daha çox cihaz arasında əlaqədir. Bu, informasiyanın şəbəkə üzərindən ötürülməsi zamanı icazəsiz girişdən, modifikasiyadan və ya ələ keçirilməsindən qoruyan müxtəlif texnologiya və protokollardan istifadə etməklə əldə edilir. Təhlükəsiz əlaqənin əsas xüsusiyyətlərinə aşağıdakılar daxildir.

- Məlumatların şifrələnməsi.
- Doğrulama.
- Verilənlərin tamlığı.
- Təkrar mühafizə.

Məlumatların Şifrələnməsi təhlükəsiz əlaqə üzərindən ötürülən bütün məlumatlar elə şifrələnir ki, yalnız səlahiyyətli alıcı onu deşifrə edə və oxuya bilər. Bu, üçüncü tərəflərin məxfi məlumatları ələ keçirməsinin və dinləməsinin qarşısını alır. Doğrulama bağlantıda iştirak edən cihazların və ya istifadəçilərin qanuniliyinin təsdiqlənməsi. Bura parollar, sertifikatlar və ya digər üsullarla autentifikasiya daxil ola bilər ki, bu, yalnız düzgün subyektlərin məlumatlara daxil olmasını təmin edir. Verilənlərin ötürülməsi zamanı dəyişdirilmədiyini və ya zədələnməməsini təmin edir. Bu, ötürmə zamanı verilənlərdə hər hansı dəyişikliyi aşkar edən hash funksiyaları və ya mesajın autentifikasiya

kodlarından (MAC) istifadə etməklə əldə edilir. Təkrar mühafizə əvvəllər ələ keçirilmiş və ya qeydə alınmış məlumat paketlərinin təkrar istifadəsini nəzərdə tutan hücumların qarşısını alır. Təhlükəsiz əlaqəni təmin edən texnologiya və protokollara misal olaraq IPSec, SSL/TLS, SSH, VPN (virtual özəl şəbəkələr) və şəbəkə rabitələrində istifadə edilən müxtəlif şifrələmə və autentifikasiya üsullarını göstərmək olar.

Şəbəkədəki son nöqtələr arasında təhlükəsiz rabitənin təmin edilməsi üçün əsasən aşağıdakı üsullardan istifadə olunur:

- IPSec protokolunun tətbiqi.
- SSH protokolunun tətbiqi.
- HTTPS SSL/TLS Təhlükəsiz Bağlantının tətbiqi.
- MPLS VPN (Multi-Protocol Label Switching Virtual Private Networks) tətbiqi.

IPSec (IP Təhlükəsizlik Protokolu) şəbəkə üzərindən ötürülən məlumatların şifrələnməsini, autentifikasiyasını və bütövlüyünü təmin edir. IPSec-in təşkilat daxilində və İnternet kimi açıq şəbəkələrdə tətbiqi trafikin məxfiliyini və bütövlüyünü qorumağa kömək edir. SSH Telnet-dən istifadə edərkən aydın mətnlə ötürülən həssas məlumatları ehtiva edən trafikin tutulmasının və təhlilinin qarşısını almaqla şəbəkə cihazlarına təhlükəsiz uzaqdan bağlantılar təmin edir. HTTPS SSL/TLS protokollarından istifadə edərək veb server və veb brauzer arasında təhlükəsiz məlumat ötürülməsinə imkan verir. Bu, müştəri və server arasında əlaqəni təhlükəsiz etmək üçün məlumat şifrələməsini, server autentifikasiyasını və anti-spoofing qorunmasını təmin edir. MPLS VPN şəbəkənin müxtəlif nöqtələri arasında əlaqə üçün təcrid olunmuş və təhlükəsiz şəbəkə mühiti təmin edir. Bu, şəbəkə daxilində məlumatların məxfiliyini və bütövlüyünü təmin edən çox protokollu etiket keçidindən istifadə edərək virtual özəl şəbəkələrin yaradılmasına imkan verir.

Bu tədbirlər kompleksi müxtəlif qurğular və şəbəkənin son nöqtələri arasında təhlükəsiz rabitə üçün hərtərəfli yanaşma təmin edir. Məlumatların tutulması, saxtakarlıq və şəbəkə daxilində hücumlar da daxil olmaqla müxtəlif növ təhlükələrdən qorunma təmin etmək üçün şifrələmə, autentifikasiya və izolyasiya kimi müxtəlif təhlükəsizlik aspektlərini nəzərə alır.

Təhlükədən qorunmaq üçün ən yaxşı təcrübələr. Güvən və şəxsiyyət vasitəsilə şəbəkə infrastrukturunu qorumaq üçün ən yaxşı təcrübələr icazəsiz girişin qarşısını almağa və riskləri minimuma endirməyə kömək edən güclü təhlükəsizlik mexanizmlərinin yaradılmasına diqqət yetirir. Bu üsullara aşağıdakılar daxildir:

- Çox faktorlu autentifikasiya.
- Parolların müntəzəm olaraq yenilənməsi və idarə edilməsi.
- Məlumatların şifrələnməsi
- Giriş və imtiyazlara nəzarət.
- Etibarlı və yenilənmiş təhlükəsizlik vasitələrindən istifadə.
- Rol əsaslı giriş nəzarəti.
- Şəbəkə seqmentasiyası.
- İstifadəçi təlimi və maarifləndirmə.
- Fəaliyyətin monitorinqi və auditi.
- Hadisəyə cavab planlarının yaradılması və sınaqdan keçirilməsi.

Çox faktorlu autentifikasiyanın həyata keçirilməsi istifadəçilərdən şəxsiyyətlərini təsdiq edən çoxsaylı sübut formalarını təqdim etmələrini tələb edir. Bu adətən parol, mobil cihaza göndərilən birdəfəlik kod və biometrik məlumatların birləşməsidir. Bu, autentifikasiya elementlərindən birinə giriş əldə etmiş olsalar belə, təcavüzkarlar üçün işi xeyli çətinləşdirir. Güclü parollardan istifadə etmək və onları müntəzəm olaraq yeniləmək icazəsiz girişin qarşısını almağa kömək edir. Sistemlər istifadəçilərdən unikal parollar yaratmağı və onların tez-tez dəyişdirilməsi siyasətini tətbiq etməyi tələb etməlidir. Həm saxlama, həm də tranzit zamanı məlumatların şifrələnməsi məlumatı ələ keçirmə və icazəsiz girişdən qorumağa kömək edir. Buraya onlayn və cihazlarda məlumatları qorumaq üçün müasir şifrələmə protokollarından istifadə daxildir. Ən az imtiyaz prinsipi istifadəçilərin və sistemlərin yalnız öz vəzifələrini yerinə yetirmək üçün lazım olan hüquqlara malik olmasını təklif edir. Bu, hüquqların pozulması riskini azaldır və potensial daxili təhdidlərin qarşısını alır.

Antivirus proqram təminatının, müdaxilənin aşkarlanması sistemlərinin (IDS) və müdaxilənin qarşısının alınması sistemlərinin (IPS) müntəzəm olaraq yenilənməsi şəbəkənizi məlum təhlükələrdən və zəifliklərdən qorumağa kömək edir. Rol əsaslı giriş nəzarətinin həyata keçirilməsi istifadəçinin təşkilatdakı roluna əsaslanaraq giriş hüquqlarını idarə etməyə imkan verir. Bu, girişə nəzarəti asanlaşdırır və istifadəçilərin yalnız öz işlərini yerinə yetirmək üçün lazım olan resurslara çıxışının olmasını təmin edir. Şəbəkənin ayrı-ayrı seqmentlərə bölünməsi girişi məhdudlaşdırmağa və şəbəkə daxilində təhlükələrin yayılmasını minimuma endirməyə kömək edir. Bu, kritik resursları və məlumatları şəbəkənin ictimai və ya daha az təhlükəsiz hissələrindən təcrid etməyə imkan verir. Mütəmadi olaraq işçilərə ən yaxşı təhlükəsizlik təcrübələri, potensial təhdidlər və müdafiə vasitələri haqqında təlim vermək insan səhvi

hücumları riskini azaltmağa kömək edir. Bura fişinq e-poçtlarının tanınması və həssas məlumatların düzgün idarə edilməsi üzrə təlim daxildir. Şəbəkə fəaliyyətinin davamlı monitorinqi və müntəzəm təhlükəsizlik auditləri anomaliyaları və şübhəli fəaliyyəti müəyyən etməyə kömək edir. Bu, potensial təhlükələrə və pozuntulara tez reaksiya verməyə imkan verir. Hadisəyə cavab planının olması və onun müntəzəm sınaqdan keçirilməsi hücumlara və digər təhlükəsizlik insidentlərinə tez və effektiv cavab verməyə kömək edir. Buraya sistemin işini bərpa etmək və zərərləri minimuma endirmək üçün prosedurların hazırlanması daxildir.

Bu üsullar və təcrübələr şəbəkə infrastrukturunuz üçün çox səviyyəli təhlükəsizlik yaratmağa, onun təhdidlərə qarşı dayanıqlığını yaxşılaşdırmağa və uğurlu hack və ya təhlükəsizlik pozuntusu ehtimalını azaltmağa kömək edir.

YOXLAMA SUALLARI

1. Şəbəkə təhlükəsizliyində məlumatların məxfiliyinə, bütövlüyünə və əlçatanlığına hansı təhlükələr var?
2. Wi-Fi simsiz şəbəkələrinə hansı növ təhlükələr tətbiq oluna bilər və onlardan qorunmaq üçün hansı tədbirləri görə bilərsiniz?
3. Şəbəkə cihazlarında hansı zəifliklər aşkar edilə bilər və riski azaltmaq üçün hansı təhlükəsizlik tədbirləri görülə bilər?
4. Şəbəkə infrastrukturunda hansı zəifliklər mövcud ola bilər və onları aşkar etmək və düzəltmək üçün hansı üsullardan istifadə etmək olar?
5. Tətbiq zəifliyindən hansı təhlükələr yarana bilər və tətbiqləri hücumlardan qorumaq üçün hansı tədbirlər görülə bilər?
6. Müxtəlif üsul və texnologiyalardan istifadə edərək onlayn təhlükəsizlik təhdidlərini necə azaltmaq olar?
7. Sistemin həyat dövrünün müxtəlif mərhələlərində hansı təhlükələr və risklər yarana bilər və onları necə idarə etmək olar?
8. Təhlükəsizlik siyasəti və prosedurları şəbəkə infrastrukturunda təhlükələrin qarşısının alınması və aşkar edilməsində hansı rolu oynayır?
9. Şəbəkə və məlumat təhlükəsizliyini təkmilləşdirmək üçün hansı autentifikasiya və şəxsiyyət idarəetmə üsullarından istifadə edilə bilər?
10. Şəbəkə təhlükəsizliyinin pozulması halında hansı nəticələr baş verə bilər və hadisədən xilas olmaq üçün hansı tədbirlər görülə bilər?

PRAKTİKİ TAPŞIRIQ

1. Evinizin Wi-Fi şəbəkəsinin təhlükəsizliyi yoxlayın.

Tapşırıq: Ev simsiz şəbəkənizin təhlükəsizlik təhlilini aparın, güclü parolların istifadəsini, marşrutlaşdırıcıda yeniləmələri və şifrələmə parametrlərini yoxlayın.

Məqsəd: Şəxsi məlumatları və cihazları potensial kiberhücumlardan qorumaq üçün ev Wi-Fi şəbəkənizi qoruyun.

2. Onlayn hesabların təhlükəsizliyinin yoxlanılması.

Tapşırıq: Məlumat sızmasının yoxlanılması xidmətlərindən və iki faktorlu autentifikasiyadan istifadə edərək onlayn hesablarınızın (məsələn, e-poçt, sosial şəbəkələr, bank hesabları) təhlükəsizliyini vaxtaşırı yoxlayın.

Məqsəd: Onlayn hesablarınızı icazəsiz girişdən və şəxsi məlumatların sızmasından qoruyun.

3.Təhlükəsizlik yeniləmələri üçün cihazların yoxlanılması.

Tapşırıq: Təhlükəsizlik yeniləmələri üçün kompüterlərinizi, mobil cihazlarınızı və digər ağıllı cihazları yoxlayın və lazım olduqda quraşdırın.

Məqsəd: Məlum zəiflikləri bağlayın və cihazları kiberhücumlardan qoruyun.

4.İşçilərə informasiya təhlükəsizliyi qaydaları üzrə təlimlərin keçirilməsi.

Məqsəd: Güclü parollardan istifadə, e-poçt qoşmalarını açarkən diqqətli olmaq və fişinq hücumlarının tanınması da daxil olmaqla, əsas informasiya təhlükəsizliyi prinsipləri üzrə işçilərə təlim vermək.

Məqsəd: İnsayder təhdidləri riskini azaltmaq və işçilərin məlumat təhlükəsizliyi təcrübələri haqqında məlumatlılığını artırmaq.

5. Binalara və cihazlara fiziki girişin təhlükəsizlik auditi.

Tapşırıq: Ofisə, server otağına və digər kritik binalara fiziki girişin təhlükəsizlik auditini aparın, o cümlədən video nəzarət sistemlərini, kilidləri, giriş sistemlərini və ziyarətçilərin monitorinqini yoxlayın.

Məqsəd: Fiziki resursları və məlumatları icazəsiz girişdən və ya oğurluqdan qoruyun.

MODUL 9. FİREWALL- ŞƏBƏKƏLƏRARASI EKRANLAŞDIRMA

FİREWALL – ŞƏBƏKƏLƏRARASI EKRANLAŞDIRMANIN ƏSAS MAHİYYƏTİ VƏ VƏZİFƏLƏRİ

FİREWALL – ƏSAS KONFİQURASİYA VƏ İŞLƏMƏ MEXANİZMİ

FİREWALL NÖVLƏRİ

PROSESLƏRİN TƏFTİŞİ VƏ PAKET FİLTRLƏMƏ

ŞƏBƏKƏ ÜNVANLARININ TRANSLYASİYASI (NETWORK ADDRESS TRANSLATİON -NAT)

YOXLAMA SUALLARI

PRAKTİKİ TAPŞIRIQ

FİREWALL – ŞƏBƏKƏLƏRARASI EKRANLAŞDIRMANIN ƏSAS MAHİYYƏTİ VƏ VƏZİFƏLƏRİ

Şəbəkələrarası ekranlaşdırmanın[44] əsas mahiyyəti təşkilatın şəbəkəsinə daxil olan və çıxan trafiki izləmək və nəzarət etməklə şəbəkə təhlükəsizliyini təmin etməkdir. Bu proses şəbəkəyə icazəsiz giriş cəhdlərini aşkar etməyə və bloklamağa, zərərli proqram təminatının yayılmasının, hücumların və məlumat sızmasının qarşısını almağa imkan verir.

- Şəbəkələrarası ekranlaşdırmanın əsas vəzifələrinə aşağıdakılar aid edilir:
- Zərərli trafikin təyini və bloklanması.
- Şəbəkə trafikinə nəzarət və filtrasiya.
- Monitorinq və hadisələrin qeydi.
- Şəbəkə ekranının mühafizəsi.
- Təhlükəsizlik siyasətləri ilə ardıcıllığı və uyğunluğu təmin edilməsi.

Firewall istifadəçiyə port skanları, xidmətdən imtina (DDoS) hücumları, viruslar, Trojan atları və zərərli proqram təminatının digər formaları kimi şəbəkəyəə müdaxilə cəhdlərini və hücumları müəyyən etməyə imkan verir. Bu, təhdidlərə tez cavab verməyə və şəbəkənizə ziyan vurmazdan əvvəl onları bloklamağa imkan verir. Firewall skrininqi sizə müəyyən edilmiş qaydalar və təhlükəsizlik siyasətləri əsasında şəbəkə trafikini idarə etməyə və filtrləməyə imkan verir. Buraya müəyyən resurslara və xidmətlərə girişin bloklanması, protokolların və proqramların istifadəsinə nəzarət, istifadəçinin və ya cihazın şəxsiyyəti əsasında şəbəkəyə girişin məhdudlaşdırılması daxildir. Firewall skrininqi şübhəli fəaliyyət və təhlükəsizlik insidentlərini müəyyən etmək üçün şəbəkə fəaliyyətinin monitorinqini və hadisələrin qeydini təmin edir. Bu, təhdidlərə tez reaksiya verməyə və hadisələrin səbəblərini və nəticələrini müəyyən etmək üçün təhlil etməyə imkan verir. Firewall skrininqi şəbəkə perimetrinin qorunmasında, xarici şəbəkələrdən icazəsiz girişin qarşısının

---

44

Келдыш Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. С.100

Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации: учеб. пособие / Н.В. Келдыш. - М.: Мир науки, 2022. – сетевое издание. Режим доступа: https://izdmn.com/PDF/14ЬТТ3Г22.pdf

Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина М.: Национальный Открытый Университет «ИНТУИТ», 2014. 378 с.

Олифер В.Г. Безопасность компьютерных сетей. М.: Горячая линия - Телеком, 2018. 644с.

alınmasında və təşkilatın daxili resurslarının xarici təhdidlərdən qorunmasında ilk müdafiə xəttini təmsil edir. Şəbəkəyə girişə və şəbəkə trafikinin işlənməsinə nəzarət etmək üçün vahid qaydalar və siyasətlər tətbiq etməklə, təhlükəsizlik divarının yoxlanılması təşkilatın təhlükəsizlik siyasətlərinə uyğunluğu təmin etməyə kömək edir. Firewall skrininqi şəbəkə təhlükəsizliyinin qorunmasında və məlumatın təhdid və hücumlardan qorunmasında əsas rol oynayır və onun həyata keçirilməsi təşkilatın ümumi informasiya təhlükəsizliyi strategiyasının mühüm tərkib hissəsidir.

FİREWALL – ƏSAS KONFİQURASİYA VƏ İŞLƏMƏ MEXANİZMİ

Firewall-ın əsas konfiqurasiyası. Firewall konfiqurasiyası şəbəkə aktivlərinin təhlükəsizliyinin vacib hissəsidir. Düzgün konfiqurasiya edilmədikdə, hətta ən güclü firewall müdafiəsi də uğursuz olacaq. Gartner təhlükəsizlik ekspertləri bildirirlər ki, firewall pozuntularının 99%-i firewall sistemlərindəki qüsurlardan deyil, yanlış konfiqurasiyadan qaynaqlanır. İstifadəçilərin firewall sistemlərini necə qurması onların ümumi təhlükəsizlik vəziyyətində böyük fərq yaradır. Bu vacibdir, çünki firewall kibertəhlükəsizlik sistemlərinin mərkəzi hissələridir. Firewalllar daxil olan və gedən şəbəkə trafikini süzgəcdən keçirir. Onlar resurslara daxil olmaq üçün yalnız təsdiqlənmiş trafikə icazə verirlər. Və onlar naməlum əlaqələri bloklayaraq, zərərli hücumçulardan qoruyurlar.

Firewalllar bu funksiyaları yalnız düzgün siyasətlə həyata keçirə bilər. **Firewall siyasətləri şəbəkəyə giriş şərtlərini bildirən təhlükəsizlik qaydaları toplusudur**. Bunlara icazə verilən portlar və təsdiq edilmiş IP ünvanları və ya domen adları daxildir. Və şəbəkəni seqmentləşdirmək üçün təhlükəsizlik zonaları tətbiq edirlər.

Bu siyasətləri düzgün əldə etmək firewall konfiqurasiyasının əsas problemidir. Filtrlər çox genişdirsə, təcavüzkarlar şəbəkəyə daxil ola bilər. Lakin həddindən artıq ciddi nəzarət qanuni istifadəçilər üçün performans problemləri ilə nəticələnə bilər. Firewall konfiqurasiyanızı necə təkmilləşdirəcəyinizi araşdıraq. Firewall konfiqurasiyası şəkil 9.1-də təsvir olunmuşdur.

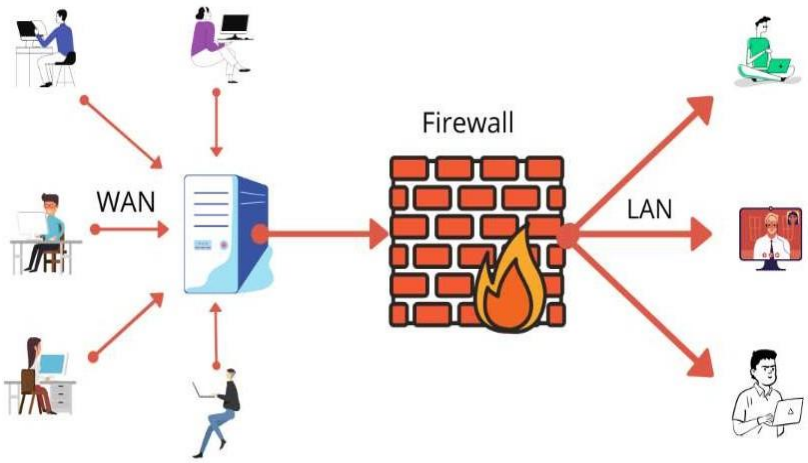
Firewall-ın konfiqurasiyası aşağıdakı ardıcıllıqla yerinə yetilir

1. Firewall təhlükəsizliyinin təmin edilməsi. Firewall konfiqurasiyası prosesində birinci mərhələ firewallun təhlükəsizliyini təmin etməkdir. Burada nəzərə alınacaq amillərə aşağıdakılar daxildir:

Defolt parolların dəyişdirilməsi - Firewalllar tez-tez hakerlərin təxmin etməsi asan olan əvvəlcədən təyin edilmiş parollarla gəlir.

Mikroproqramın yenilənməsi - Köhnəlmiş proqram istismara qarşı həssasdır. Ən son yamalar təhlükəsizlik boşluqlarını aradan qaldıracaq.

Sadə Şəbəkə İdarəetmə Protokolu (SMTP) - SMTP aktivdirsə, onu söndürün. Bunun səbəbi SMTP-nin ən son autentifikasiya sistemlərini dəstəkləməməsidir. Təcavüzkarlar istifadəçiləri aldada və şəbəkə xidmətlərinə giriş əldə edə bilərlər.



Şəkil 9.1. Firewall-ın əsas konfiqurasiyası

TCP trafik tənzimlənməsi - Transmissiya İdarəetmə Protokolundan istifadə edərək daxil olan və gedən trafiki məhdudlaşdırın. Təcavüzkarlar üçün giriş marşrutlarını bağlamaq üçün mümkün qədər az portu aktivləşdirin.

İstifadə edilməmiş açıq portların bağlanması - Məsələn, FTP portları (adətən Port 21) mümkün olduqda bağlı qalmalıdır.

2. İstifadəçi hesablarını idarə edin.

Firewall parametrlərinə girişi olan istifadəçilərin düzgün konfiqurasiya olunduğundan əmin olun. Birdən çox administrator üçün paylaşılan hesabların istifadəsindən çəkinin. Paylaşılan istifadəçi hesabları xarici təcavüzkarlar üçün cazibədar bir hədəfdir. Bunun əvəzinə, hər bir inzibati səviyyəli istifadəçi üçün

fərdi hesablar qurun.Ümumi nəzarəti bir istifadəçiyə təyin etməyin. Təminatlar

yaratmaq üçün Rol Əsaslı Giriş Nəzarəti (RBAC) vasitəsilə istifadəçi imtiyazlarını ayırın . Bu, hakerlərin admin hesabını ələ keçirməsi halında zərəri məhdudlaşdırır. Firewall konfiqurasiyasını həyata keçirərkən hər şeyi düzgün əldə etsəniz, təcavüzkarlar hələ də yüksək imtiyazlı hesabları poza bilər. Admin istifadəçilərinin ciddi parol gigiyenasına riayət etmələrini təmin etmək üçün əlavə diqqətli olun. İstənilən standart parolları dəyişdirin və müntəzəm olaraq dəyişdirilən təhlükəsiz parolları tələb edin.

3. Şəbəkə aktivlərini qorumaq üçün firewall zonalarından istifadə edin. Firewall zonaları **yüksək dəyərli məlumat və aktivləri ehtiva edən şəbəkə sahələridir**. Firewalllar bu şəbəkə zonalarını əhatə edərək səlahiyyətli istifadəçilərə giriş imkanı verir. Bu, PCI-DSS qaydalarına cavab verən etibarlı şəbəkə təhlükəsizliyi vasitəsidir. Hər bir firewall zonasına hansı resursların təyin ediləcəyini diqqətlə nəzərdən keçirin. Həmişə biznes ehtiyaclarını ön planda tutun və resursları ağıllı şəkildə qruplaşdırın.

Şəbəkə zonası strukturu yaratarkən, mürəkkəbliyin xərclərinin olduğunu unutmayın. Daha çox zona ümumi təhlükəsizliyi artıracaq. Lakin adminlər seqmentləşdirilmiş zonaları idarə etməyə vaxt ayırmalıdırlar. Bu kiçik təşkilatlarda problem ola bilər. E-poçt serverləri, veb serverlər və Virtual Şəxsi Şəbəkə (VPN) serverləri də daxil olmaqla, **kritik serverlər üçün silahsızlaşdırılmış zona yaratmaq** yaxşı təcrübədir. Bu, əsas resurslardan uzaqda dərin monitorinq etməyə imkan verən şəbəkəyə daxil olan və çıxan trafiki ehtiva edir.

Firewall zonası infrastrukturu haqqında da düşünün. Hər bir zona hər bir firewall interfeysini düzgün zona ilə birləşdirən IP ünvanı strukturu tələb edir.

4. Girişə Nəzarət Siyahılarını (ACL) qurun.

Girişə nəzarət siyahıları şəbəkəyə hansı növ trafikin daxil olduğunu təyin edən təhlükəsizlik divarı qaydalarıdır. Onlar əsasən şəbəkə qonaq siyahısı kimi çıxış edirlər. Girişə nəzarət siyahılarını konfiqurasiya etdiyiniz zaman kimin qəbul ediləcəyini və kimin xaric ediləcəyini özünüz qərar verirsiniz.

Firewall sistemindəki hər bir alt-interfeys əsas firewall yönləndiricisi ilə birlikdə öz ACL-yə malik olmalıdır. ACL-də ümumi firewall qaydalarına aşağıdakılar daxildir:

- Mənbə port nömrələri.
- Təyinat port nömrələri.
- İcazə verilən internet protokolu (IP) ünvanları.
- İcazə verilən protokollar, o cümlədən IP, EDP və ya TCP.

- Sonda təsdiqlənməmiş şəxsiyyətlərə girişi rədd edən "hamısını rədd et" qaydası.

Administratorlar həmçinin **firewall idarəetmə interfeyslərini qorumalıdırlar**. Nəzarət sisteminə ictimai girişi bloklayın və şifrələnməmiş firewall idarəetmə protokollarını deaktiv edin.

5. Firewall konfiqurasiyanızın uyğun olduğundan əmin olun.

Firewall qorunması **PCI-DSS və HIPAA kimi qaydaların vacib hissəsidir** . Uyğunluğa nail olmaq üçün təşkilatlar müştəri və ya pasiyent məlumatları ətrafında möhkəm firewall quraşdırmalıdırlar. Hər hansı konfiqurasiya dəyişikliyinin tənzimləyici standartlara cavab verdiyinə əmin olun. Mümkünsə, konfiqurasiyanızı müvafiq qaydalar ətrafında qurun. Qeydiyyat PCI-DSS altında əsas tələbdir. Şirkətlər **giriş sorğularını daxil etmək və saxlamaq imkanı olan firewall qurmalıdırlar** . Avtomatlaşdırılmış girişin aktiv olduğundan əmin olun. Və audit funksiyasının dəqiq, hərtərəfli məlumatları təqdim etdiyini iki dəfə yoxlayın.

6. Firewall müdafiənizi sınayın və yoxlayın.

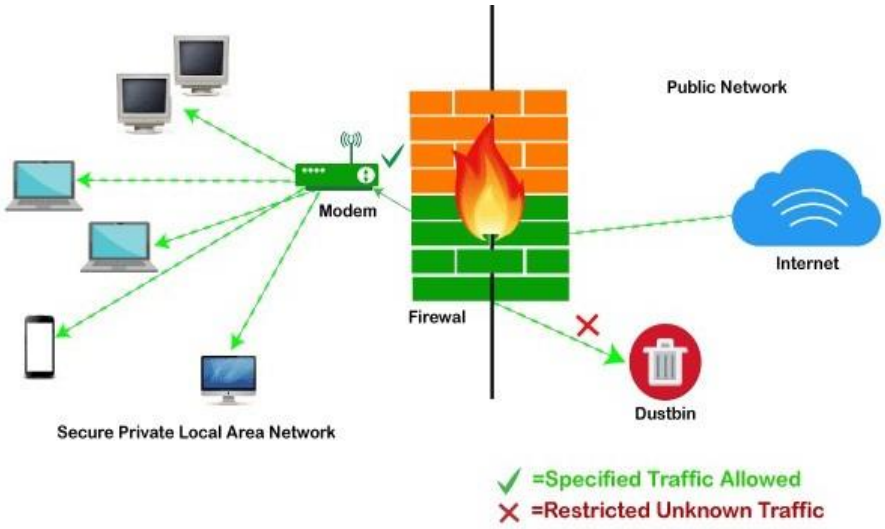
Konfiqurasiya zamanı **zəiflikləri yoxlamaq üçün nüfuz testindən və zəiflik skanından istifadə edin**. Test təkmilləşdirmə sahələrini müəyyənləşdirir. Bu, firewall işə başlamazdan əvvəl təhlükəsizlik problemlərini həll etməyi asanlaşdırır. Müvafiq təhlükəsizlik yoxlamaları aparmadan heç vaxt firewall-u aktivləşdirməyin. Yerləşdirmədən sonra **audit kritik əhəmiyyət kəsb edir**. Firewall qeydlərini yoxlamaq və növbəti boşluq skanlarını həyata keçirmək üçün auditlər planlaşdırın. ACL və qaydaların müvafiq və təhlükəsiz olduğuna əmin olun. İstənilən dəyişiklikləri sənədləşdirin və tənzimləyici hesabatları asanlaşdırmaq üçün audit məlumatlarını saxlayın. Firewall proqram təminatını yeniləmək üçün prosedurları yerinə yetirin. Avtomatlaşdırma yamaqları minimal inzibati girişlə çatdıra bilər. Lakin proqram təminatının güncəl olub olmadığını yoxlamaq vacibdir. Və unutmayın: Yamalar zəiflik skanlarını lazımsız etmir.

Firewall-ın işləmə mexanizmi. Firewallun işləmə mexanizmi şəbəkə təhlükəsizliyini təmin etmək üçün şəbəkə trafikinin süzülməsi və idarə edilməsi prinsiplərinə əsaslanır(şəkil 9.2).

Şəkildən göründüyü kimi, Firewallun işləməsinin ümumi mexanizmi aşağıdakı kimi təşkil olunur:

- Firewall-un ilk addımı ondan keçən şəbəkə məlumat paketlərini təhlil etməkdir. Bu, mənbə və təyinat IP ünvanları, portlar və protokol kimi

parametrləri müəyyən etmək üçün paket başlıqlarının araşdırılmasını əhatə edir.



Şəkil 9.2. Firewall-ın iş prinsipi

- Məlumat paketi parametrlərinə və təhlükəsizlik qaydaları və şəbəkə siyasəti kimi digər amillərə əsaslanaraq, firewall bir sıra trafik filtrləmə qaydaları tətbiq edir. Bu qaydalar hansı trafikə icazə verildiyini və nəyin bloklandığını müəyyən edir.

- Bəzi firewalllar yalnız paket başlıqlarını deyil, həm də onların məzmununu və şəbəkə əlaqələrinin vəziyyətini yoxlayan vəziyyəti təsdiqləyən yoxlama texnikasından istifadə edir. Bu, təhlükəsizlik divarına kontekst əsasında trafikin keçməsi və ya bloklanması ilə bağlı qərarlar qəbul etməyə imkan verir.

- Konfiqurasiya edildikdə, firewall şəbəkə paketlərindəki mənbə və/yaxud təyinat IP ünvanlarını və portlarını yenidən yazmaqla NAT-ı yerinə yetirir. Bu, daxili şəbəkə ünvanlarını xarici dünyadan gizlətmək və ya vahid ümumi xarici ünvan vasitəsilə xarici resurslara çıxışı təmin etmək üçün faydalı ola bilər.

-Firewall işlədikcə hadisə qeydlərini saxlayır, ondan keçən trafik, qəbul edilmiş qərarlar və potensial təhlükələr haqqında məlumatları qeyd edir. Bu qeydlər şəbəkə fəaliyyətini təhlil etmək və potensial təhlükəsizlik problemlərini və ya insidentləri müəyyən etmək üçün istifadə edilə bilər.

- Parametrlərdən və aşkar edilmiş təhdidlərdən asılı olaraq, firewall əlaqələri bloklamaq, şəbəkə administratorlarına xəbərdarlıq göndərmək və ya filtrləmə qaydalarını avtomatik tənzimləmək kimi müxtəlif cavab tədbirləri görə bilər.

Ümumiyyətlə, firewall mexanizmi müəyyən edilmiş təhlükəsizlik siyasəti və qaydalarına uyğun olaraq şəbəkə trafikinə nəzarət və filtrasiya yolu ilə şəbəkə təhlükəsizliyini təmin etməyə yönəlib.

FİREWALL NÖVLƏRİ

Hər biri xüsusi ehtiyacları və şəbəkə təhlükəsizliyi ehtiyaclarını qarşılamaq üçün nəzərdə tutulmuş bir neçə növ firewall mövcuddur:

- Proqram (Software) firewalllar.
- Aparat (Hardware) firewallları.
- Virtual firewalllar.

Proqram təminatının firewalllar adi server və ya kompüterdə quraşdırılan və işləyən proqram təminatı kimi fəaliyyət göstərir. Proqram təminatının təhlükəsizlik duvarları adətən geniş funksiyalar və konfiqurasiya çevikliyi təmin edir, lakin işləmək üçün aparat resursları tələb edir. Buna misal olaraq Windows Firewall, Windows əməliyyat sistemləri ailəsinə daxil edilmiş proqram təhlükəsizlik divarını göstərmək olar. O, kompüterə icazəsiz girişə qarşı əsas müdafiəni təmin edir və təhlükəsizlik parametrlərinizə uyğun olaraq şəbəkə trafikinə nəzarət edir.

Aparat (Hardware) firewall şəbəkə təhlükəsizliyini təmin etmək üçün xüsusi olaraq hazırlanmış fiziki cihazlardır. Onlar adətən xüsusi aparat komponentləri vasitəsilə yüksək performans və etibarlılıq təmin edir. Hardware firewallları tez-tez böyük təşkilatlarda və məlumat mərkəzlərində istifadə olunur. Buna misal olaraq Cisco ASA (Adaptive Security Appliance) şəbəkə və VPN bağlantıları üçün təhlükəsizliyi təmin etmək üçün nəzərdə tutulmuş hardware firewalları göstərmək olar. O, yüksək performansa və genişlənmə qabiliyyətinə malikdir və dərin paket yoxlaması və proksiinq daxil olmaqla geniş spektrli təhlükəsizlik xüsusiyyətlərini dəstəkləyir.

Virtual Firewall virtual maşınlar və ya bulud xidmətləri kimi virtuallaşdırılmış mühitlərdə işləyən proqram həlləridir. Onlar virtual

şəbəkələrin və resursların qorunmasını təmin edir, konfiqurasiya çevikliyinə və genişlənmə qabiliyyətinə malikdir.

Virtual təhlükəsizlik divarları fiziki təhlükəsizlik divarını hər birinin öz konfiqurasiyası olan çoxlu məntiqi qurğulara bölmək üçün istifadə olunan təhlükəsizlik kontekstləridir. Bu, birdən çox müstəqil təhlükəsizlik divarına sahib olmağa bənzəyir, lakin ayrı-ayrı cihazlar satın almadan. Cihazda təhlükəsizlik kontekstlərini təyin edərkən köhnə konfiqurasiya müvafiq faylda saxlanacaq və yeni virtual təhlükəsizlik divarlarının hər birində xüsusi konfiqurasiya faylları olacaq.

Təhlükəsizlik kontekstləri aşağıdakılar kimi öz atributlarına malik olmaq mənasında fərqli və müstəqil firewalllardır:

- Təhlükəsizlik siyasəti.
- Təyin edilmiş interfeyslər.
- NAT qaydaları.
- Girişə nəzarət siyahıları.
- Administratorlar.

Hər bir virtual təhlükəsizlik divarının inzibatçı konteksti vasitəsilə dəyişdirilə bilən sistem konfiqurasiyası var, siz tək rejimdən çox rejimə çevirdiyiniz zaman avtomatik olaraq yaradılır. Sistemə daxil olmaq və onu konfiqurasiya etmək üçün istifadə edildiyi istisna olmaqla, administrator konteksti əsasən hər hansı digər virtual firewall kimidir. Tipik olaraq dizaynda VLAN-lar təhlükəsizlik kontekstləri ilə əlaqələndiriləcək və əksər firewalllar birdən çox VLAN-ın tək təhlükəsizlik kontekstinə təyin edilməsinə imkan verir.

Ümumi virtual firewalllar tərəfindən ümumiyyətlə dəstəklənməyən bəzi şeylərə aşağıdakılar daxildir:

- IPSec VPN.
- SSL VPN.
- Dinamik marşrutlaşdırma protokolları.

Virtual firewall dizaynına gəldikdə başqa bir vacib konsepsiya resurs siniflərini əhatə edir. Təhlükəsizlik cihazını konfiqurasiya edərkən, defolt olaraq, bütün resurslar bütün təhlükəsizlik kontekstləri üçün əlçatandır. Bu, administrator kontekstində dəyişdirilə bilər ki, bu da sizə yeni kontekstlər yaratmağa və onların hər birinə resurslar təyin etməyə imkan verəcək. Bu resurslar asan idarə olunmaq üçün resurs siniflərində qruplaşdırıla bilər və onlara administrator konteksti vasitəsilə təhlükəsizlik kontekstləri təyin edilə bilər.

Bu tip firewallların hər birinin öz üstünlükləri və mənfi cəhətləri var və konkret növün seçilməsi təşkilatın ehtiyaclarından, büdcəsindən, şəbəkə ölçüsündən və digər amillərdən asılıdır. Məsələn, hardware firewallları yüksək performans tələbləri olan böyük müəssisələr üçün, virtual firewall isə bulud mühitləri və orta ölçülü müəssisələr üçün daha uyğun ola bilər.

PROSESLƏRİN TƏFTİŞİ VƏ PAKET FİLTRLƏMƏ

Firewall bir neçə rejimdə işləyə bilər. Köhnə iş rejimi paket filtrasiyası kimi də tanınan vətəndaşsız təhlükəsizlik divarıdır. Bu texnika xüsusi məlumatların daxil olmasına icazə vermək və xüsusi məlumatları şəbəkədən kənarda saxlamaq üçün təhlükəsizlik duvarını qaydalarla konfiqurasiya etməyi əhatə edir. Daxil olan və çıxan məlumatların bir-biri ilə heç bir əlaqəsi yoxdur, çünki firewall yalnız hər iki tərəfdən portları açır və ya IP ünvanları əsasında girişi məhdudlaşdırır. Müasir firewalllar paket yoxlamasını təklif edir, yəni cihazdan keçən bütün axınları başa düşür və izləyir. Onlar yalnız xüsusi cihazlar arasında, məsələn, müxtəlif müştərilər və server arasında trafikin axmasına imkan verir. Bunun funksiyası hər bir əlaqənin vəziyyətini (axınlar və ardıcıllıq nömrələri) qeyd etmək və bu əlaqə ilə əlaqəli cavablara avtomatik icazə verməkdən ibarətdir. Məsələn, siz təhlükəsizlik divarını 80-ci porta trafikə icazə vermək üçün konfiqurasiya edə bilərsiniz. Bu halda sizə hər hansı bir geri qayıdış trafiki qaydasını təyin etməli deyilsiniz, çünki bunlar veb serverlərdən cavabın geri qaytarılmasına icazə vermək üçün firewall (daxili olaraq) tərəfindən avtomatik olaraq yaradılır. müştərilər.

Firewall qaydaları. Firewalllar əvvəlcədən müəyyən edilmiş qaydalar toplusuna əsaslanaraq şəbəkə trafikini izləmək və filtrləməklə şəbəkə təhlükəsizliyində əsas rol oynayır. Varsayılan olaraq, firewalllar tez-tez şəbəkəni icazəsiz giriş və təhdidlərdən qorumaq üçün bütün gələn və gedən trafiki bloklayır. Müəyyən trafik növlərinə icazə vermək və şəbəkənin funksionallığını təmin etmək üçün firewalldan hansı trafikin keçə biləcəyini müəyyən edən qaydaların siyahısını yaratmalısınız. Firewalllar adətən dəyişənlər qrupları olan tuple kimi tanınan qaydalardan istifadə edərək işləyir:

- IP mənbəyi.
- IP təyinatı.
- Port nömrəsi.

- Tətbiq.
- Paket ölçüsü.
- Günün vaxtları

Mənbə IP parametri şəbəkə trafikinin gəldiyi cihazın ünvanını göstərir. Qaydalar mənbə IP ünvanları əsasında trafikə icazə vermək və ya bloklamaq üçün konfiqurasiya edilə bilər ki, bu da sizə xüsusi yerlərdən və ya şəbəkələrdən şəbəkəyə girişi idarə etməyə imkan verir. IP Təyinatı parametri şəbəkə trafikinin yönəldildiyi ünvanı təyin edir. IP təyinatının filtrlənməsi sizə şəbəkədəki müəyyən serverlərə və ya xidmətlərə girişi məhdudlaşdırmağa, bu ünvanlara yönəldilmiş trafiki bloklamağa və ya icazə verməyə imkan verir. Port nömrəsi hansı xidmətlərin və ya proqramların şəbəkə trafikindən istifadə etdiyini müəyyən edir. Qaydalar, məsələn, veb serverlər və ya poçt serverləri kimi icazə verilən xidmətlər üçün istifadə edilməyən portlara bütün əlaqələri bloklamağa imkan verən trafiki port nömrəsinə görə filtrləmək üçün konfiqurasiya edilə bilər. Bəzi firewalllar onu yaradan proqramların növünə əsasən trafiki süzgəcdən keçirə bilər. Bu, yalnız HTTP-yə icazə vermək və bütün digər proqram növlərini bloklamaq kimi hansı növ proqramların firewall vasitəsilə əlaqə saxlaya biləcəyinə daha ətraflı nəzarət etməyə imkan verir. Paket ölçüsü parametri şəbəkə paketlərinin ölçüsünə aiddir. Paket ölçüsünün filtrasiyası sizə müəyyən ölçüləri aşan paketlərlə trafiki bloklamağa imkan verir ki, bu da paket həddən artıq yükləmə hücumları kimi müəyyən növ hücumlardan qorunmaq üçün faydalı ola bilər. Günün vaxtı girişə nəzarət etmək üçün günün vaxtı həmçinin təhlükəsizlik duvarı qaydalarında istifadə edilə bilər. Bu, müəyyən saatlarda resurslara girişi məhdudlaşdırmaq, məsələn, iş saatları ərzində şəbəkəyə girişi idarə etmək və qeyri-iş saatlarında onları bloklamaq üçün faydalı ola bilən vaxta əsaslanan trafik filtrasiyasını konfiqurasiya etməyə imkan verir. Bu parametrlər şəbəkə infrastrukturu üçün çevik və fərdiləşdirilə bilən mühafizəni təmin edərək, firewalllara hansı trafikə icazə vermək və nəyi bloklamaq barədə qərar qəbul etməyə kömək edən dəstlər yaratmaq üçün birləşir.

ŞƏBƏKƏ ÜNVANLARININ TRANSLYASİYASI (NAT)

Şəbəkə Ünvanının Translyasiyası (NAT)[45] TCP/IP şəbəkələrində IP ünvanlarının bir ünvan sahəsindən digərinə tərcüməsi prosesidir. NAT-ın əsas ideyası marşrutlaşdırıcıdan və ya firewalldan keçən şəbəkə paketlərindəki mənbə və/və ya təyinat IP ünvanlarını və portlarını dəyişdirməkdir. Bu, daxili ünvanları gizlətməyə və xarici şəbəkələrə təhlükəsiz qoşulma təmin etməyə, həmçinin ictimai IP ünvanlarının məhdud resurslarından səmərəli istifadə etməyə imkan verir. NAT-ın əsas vəzifələrinə aşağıdakılar daxildir:

- Daxili IP ünvanlarının gizlədilməsi.
- IPv4 ünvanlarına dəstək.
- Trafikə və təhlükəsizliyə nəzarət.
- Çoxlu əlaqəni dəstəkləyir.
- Şəffaf proksi və yük balansın xüsusiyyətlərinin təyini.

NAT-ın əsas məqsədlərindən biri lokal şəbəkədəki cihazların daxili IP ünvanlarını İnternet kimi xarici şəbəkələrdən gizlətməkdir. Daxili IP ünvanlarını xarici şəbəkə vasitəsilə ötürmək əvəzinə, NAT onları bir (və ya daha çox) ictimai IP ünvanları ilə əvəz edir. NAT istifadəçiyə məhdud resurslar olan ictimai IPv4 ünvanlarını saxlamağa imkan verir. Daxili ünvanları bir və ya bir neçə ictimai IP ünvanına çevirməklə, NAT yerli şəbəkədə çoxlu sayda cihazlara İnternetə çıxışı təmin etmək üçün daha az ümumi ünvandan istifadə etməyə imkan verir. NAT IP ünvanları və portlar əsasında şəbəkə trafikini filtrləmək və ya yönləndirmək yolu ilə təhlükəsizlik və trafikə nəzarət siyasətlərini həyata keçirməyə imkan verir. Bu, şəbəkə resurslarına girişi idarə etməyə və şəbəkəni xarici təhlükələrdən qorumağa imkan verir. NAT-dan istifadə edərək, siz yerli şəbəkənizdəki birdən çox cihazı bir ümumi ictimai IP ünvanı vasitəsilə İnternetə qoşa bilərsiniz. Bu xüsusilə ev şəbəkələri və ya kiçik ofislər üçün faydalıdır, burada yalnız bir xarici IP ünvanından istifadə edərək birdən çox cihaza İnternetə çıxış təmin etməlisiniz. Bəzi NAT tətbiqləri şəbəkə performansını

45

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. М.: Форум, Инфра-М, 2017. 416 с.

Ярочкин, В. Безопасность информационных систем / В. Ярочкин. М.: Ось-89, 2016. 320 с.

Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с

və etibarlılığını yaxşılaşdırmaq və trafiki çoxsaylı çıxış linkləri arasında yaymaq üçün şəffaf proxy və yük balanslaşdırma xüsusiyyətlərini dəstəkləyir. NAT-ın əsas konfiqurasiyası və onun necə işləməsi istifadə olunan aparat və ya proqram təminatından asılı olaraq dəyişə bilər. NAT-ın işləmə mexanizmi aşağıdakı kimi təşkil olunur:

Ünvan tərcüməsi.

Bağlantının izlənməsi.

Tərs ünvan tərcüməsi.

Lokal şəbəkədəki cihazdan paket qəbul edərkən, NAT xarici şəbəkəyə göndərməzdən əvvəl paketin mənbə IP ünvanını və portunu ümumi IP ünvanına və portuna dəyişir. Bu proses Source NAT və ya NAT Overload adlanır (NAT həddən artıq yüklənməsi bir ictimai IP ünvanından istifadə edərək birdən çox əlaqəni idarə etmək üçün istifadə olunur). Xarici host daxili cihazlardan gələn sorğulara cavab verdikdə, ünvanları və portları düzgün tərcümə etmək üçün NAT hər bir şəbəkə bağlantısının vəziyyətinə nəzarət edir. NAT xarici cihazlardan cavab paketlərini qəbul edərkən xarici IP ünvanlarını və portlarını da nəzarət edir və onları daxili IP ünvanlarına və portlarına çevirir.

YOXLAMA SUALLARI

Firewall nədir və şəbəkə təhlükəsizliyində onun əsas məqsədi nədir?

Firewall tərəfindən yerinə yetirilən məsuliyyətlər və şəbəkə yoxlama tapşırıqları hansılardır?

Firewallların hansı növləri var və onlar bir-birindən nə ilə fərqlənir?

Əsas firewall konfiqurasiyası necə edilir və adətən hansı əsas parametrlər konfiqurasiya edilir?

Firewallda paket yoxlama mexanizmi necə işləyir?

Firewall hansı paket filtrləmə üsullarından istifadə edə bilər və onlar şəbəkə təhlükəsizliyinə necə təsir edir?

Şəbəkə Ünvanının Tərcüməsi (NAT) nədir və o, firewall ilə qorunan şəbəkələrdə necə istifadə olunur?

Şəbəkə Ünvan Tərcüməsinin (NAT) üstünlükləri və çatışmazlıqları hansılardır?

Şəbəkəni qorumaq üçün firewall tərəfindən şəbəkə trafikinə hansı növ yoxlamalar və filtrasiya tətbiq oluna bilər?

Hansı texnika və üsullar firewall hücumlarını aşkar etməyə və qarşısını almağa kömək edə bilər?

Şəbəkənin seqmentləşdirilməsində və daxili təhdidlərdən qorunmasında firewallun rolu nədir?

Müəyyən bir şəbəkə üçün firewall növünü seçərkən hansı amilləri nəzərə almalısınız?

Firewalllar müdaxilənin aşkarlanması sistemləri (IDS) və müdaxilənin qarşısının alınması sistemləri (IPS) kimi digər şəbəkə təhlükəsizlik vasitələri ilə necə qarşılıqlı əlaqədə ola bilər?

Şəbəkə təhlükəsizliyi üçün səhv konfiqurasiya edilmiş və ya qeyri-kafi firewall hansı nəticələrə səbəb ola bilər?

Firewall şəbəkə performansına necə təsir edə bilər və onları konfiqurasiya edərkən və istifadə edərkən necə nəzərə alınır?

PRAKTİKİ TAPŞIRIQ

1. Firewall konfiqurasiyasını yoxlayın və onun parametrlərinin təhlükəsizlik tövsiyələrinə uyğun olduğunu yoxlayın.

Tapşırıq: Firewall konfiqurasiyasının auditinin aparılması.

Məqsəd: Firewall parametrlərinizin təhlükəsizlik tövsiyələrinə uyğun olduğundan əmin olun.

2. Müəyyən portlara və ya protokollara girişi bloklayan təhlükəsizlik duvarında trafik filtrləmə qaydalarını konfiqurasiya edin.

Tapşırıq: Firewallda trafik filtrləmə qaydalarının konfiqurasiyası.

Məqsəd: Şəbəkə təhlükəsizliyini artırmaq üçün müəyyən portlara və ya protokollara girişi bloklayan qaydalar yaradın.

3. Firewallda NAT mexanizminin işini yoxlayın və onun şəbəkə təhlükəsizliyinə təsirini qiymətləndirin.

Tapşırıq: Firewallda NAT mexanizminin işinin yoxlanılması.

Məqsəd: NAT mexanizminin fəaliyyətini və onun şəbəkə təhlükəsizliyinə təsirini qiymətləndirin.

4. Audit jurnallarından istifadə edərək, şəbəkəyə daxil olmaq üçün icazəsiz cəhdləri müəyyənləşdirin və bloklayın.

Məqsəd: Şəbəkəyə giriş üçün icazəsiz sorğuları müəyyən edin və bloklayın. Məqsəd: Audit qeydlərindən istifadə edərək, təhlükəsizlik təhdidlərinin qarşısını almaq üçün icazəsiz şəbəkəyə giriş cəhdlərini aşkar edin və bloklayın.

5. Firewall quraşdırılmasından əvvəl və sonra gecikmə və ötürmə qabiliyyətini ölçməklə firewall tətbiqinin şəbəkə performansına təsirini qiymətləndirin.

Məqsəd: Firewall tətbiqinin şəbəkə performansına təsirini qiymətləndirin.

Məqsəd: performansa təsirini müəyyən etmək üçün firewall quraşdırmadan əvvəl və sonra şəbəkə gecikməsini və ötürmə qabiliyyətini ölçmək.

MODUL 10. MAS (IDS)/MQS (IPS) SİSTEMLƏRİ

MAS (IDS)/MQS (IPS) SİSTEMLƏRİNƏ GİRİŞ
MAS (IDS) İŞLƏMƏ MEXANİZMİ VƏ NÖVLƏRİ
MQS (IPS) İŞLƏMƏ MEXANİZMİ VƏ NÖVLƏRİ
MAS (IDS) ilə MQS (IPS) ARASINDAKI FƏRQ
SIEM - HADİSƏ VƏ MƏLUMATLARIN TƏHLÜKƏSİZ İDARƏETMƏ SİSTEMLƏRİ
ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN ƏMƏLİYYAT MƏRKƏZİ

YOXLAMA SUALLARI
PRAKTİKİ TAPŞIRIQ

MAS (IDS)/MQS (IPS) SİSTEMLƏRİNƏ GİRİŞ

Müasir informasiya texnologiyalarında kibertəhlükəsizliyin təmin edilməsində müdaxilənin aşkarlanması sistemləri (IDS) və müdaxilənin qarşısının alınması sistemləri (IPS) əsas rol oynayır. Kibertəhlükələrin sayının artması və mürəkkəbliyi ilə təşkilatlar getdikcə öz informasiya sistemlərini icazəsiz girişdən, hücumlardan və məlumat sızmasından qorumaq ehtiyacı ilə üzləşirlər. Bu kontekstdə IDS və IPS şəbəkə infrastrukturunun monitorinqi, təhlili və mühafizəsi üçün əvəzsiz alətlərə çevrilib. Hər il kiberhücumların sayı artır və onlar daha da mürəkkəbləşir. Zərərli proqram, fişinq, DDoS hücumları və digər hakerlik üsulları həm maliyyə, həm də reputasiya baxımından ciddi ziyan vura bilər. Belə şəraitdə müdaxilələrin vaxtında aşkarlanması və qarşısının alınmasının əhəmiyyəti xüsusilə kəskinləşir. Bulud hesablamalarının, Əşyaların İnternetinin (IoT) və 5G şəbəkələrinin inkişafı ilə İT infrastrukturları getdikcə daha mürəkkəb və bir-biri ilə əlaqəli olur. Bu, potensial təcavüzkarlar üçün daha təkmil və effektiv təhlükəsizlik texnikası tələb edən yeni boşluqlar və giriş nöqtələri yaradır.

Bir çox ölkə və regionlar ciddi kibertəhlükəsizlik qaydaları və standartları tətbiq edirlər. Məsələn, Avropada GDPR və ABŞ-da NIST təşkilatlardan məlumat və sistemləri qorumaq üçün tədbirlər görməyi tələb edir. Müasir IDS və IPS tətbiq etmədən bu tələblərə cavab vermək çox vaxt mümkün deyil.

Kiberhücumlar əhəmiyyətli iqtisadi itkilərə səbəb ola bilər. Hackdən sonra bərpa xərcləri, məlumat sızması üçün cərimələr, dayanma müddətindən yaranan itkilər - bütün bunlar müdaxilənin aşkarlanması və qarşısının alınması sistemlərinə sərmayə qoymağı iqtisadi cəhətdən mümkün edir. Müasir IDS və IPS maşın öyrənməsi, süni intellekt və böyük verilənlərin analitikası kimi qabaqcıl texnologiyalardan istifadə edərək anomaliyaları və təhlükələri daha effektiv müəyyən etməyə imkan verir. Bu texnologiyaların daim təkmilləşdirilməsi IDS və IPS-i informasiya sistemlərinin qorunması üçün daha vacib alətlər edir.

Beləliklə, müdaxilənin aşkarlanması və qarşısının alınması sistemləri müasir kibertəhlükəsizliyin kritik komponentləridir və kibertəhlükələr artdıqca və İT infrastrukturları mürəkkəbləşdikcə onların aktuallığı artmağa davam edir. [46]

[46] https://www.howtonetwork.com/comptia-network-study-guide-free/

Müdaxilənin aşkarlanması sistemləri (Intrusion Detection Systems (IDS)) şübhəli və ya zərərli fəaliyyəti müəyyən etmək üçün şəbəkə trafikini və sistem hadisələrini izləmək üçün nəzərdə tutulmuşdur. İDS-in əsas vəzifəsi informasiya sisteminin təhlükəsizliyinə təhlükə yarada bilən icazəsiz giriş cəhdlərini, hücumları və digər anomal fəaliyyətləri vaxtında aşkar etməkdir. IDS-in əsas komponentlərinə daxildir:

- Trafik monitorinqi və təhlili.
- Anomaliya aşkarlanması.
- Xəbərdarlıq və hesabat.
- Hadisələrin qeydiyyatı.

Trafik monitorinqi və təhlili – IDS davamlı olaraq şəbəkə trafikinə nəzarət edir və onu müdaxilə əlamətləri üçün təhlil edir. Buraya məlumat paketlərinin, sistem və proqram qeydlərinin təhlili daxildir.

Anomaliya aşkarlanması – İmza və anormal analiz üsullarından istifadə edərək, IDS şübhəli fəaliyyətləri aşkar edə bilər. İmza təhlili trafiki məlum təhlükələrin verilənlər bazası ilə müqayisə edir, anomal analiz isə normal sistemin davranışından kənara çıxmalara baxır.

Xəbərdarlıq və hesabat – Şübhəli fəaliyyət aşkar edildikdə, IDS xəbərdarlıqlar yaradır və sistem administratorları üçün hesabatlar yaradır ki, bu da onlara mümkün təhlükələrə tez cavab verməyə imkan verir.

Hadisələrin qeydiyyatı – Bütün aşkar edilmiş hadisələr və şübhəli fəaliyyətlər hadisələrin sonrakı təhlili və araşdırılması üçün jurnal fayllarında qeyd olunur.

IDS-in əsas funksiyalarına aşağıdakılar daxildir:

- Erkən təhlükənin aşkarlanması.
- Hadisənin təhlili və araşdırılması.
- Təhlükəsizlik siyasəti dəstəyi.
- Riskin azaldılması.
- Təlim və təkmilləşdirmə.

IDS təhlükələri erkən mərhələlərində aşkar etmək, potensial hücumları ciddi ziyan vurmazdan əvvəl qarşısını almaq üçün nəzərdə tutulub. IDS tərəfindən yaradılan qeydlər və hesabatlar insidentin təhlili və təhqiqatı üçün dəyərli məlumat mənbəyi kimi xidmət edir, hücumun xarakterini və mənbəyini müəyyən etməyə kömək edir. IDS təşkilatlara giriş qaydalarını və digər qaydaları pozmaq cəhdlərini aşkar edərək təhlükəsizlik siyasətlərini tətbiq etməyə kömək edir. Təhlükələrin vaxtında müəyyən edilməsi və onlara cavab verilməsi məlumat itkisi, maliyyə itkiləri və təşkilatın reputasiyasının

zədələnməsi risklərini əhəmiyyətli dərəcədə azalda bilər. IDS-dən əldə edilən məlumatlar işçiləri öyrətmək və mövcud təhlükəsizlik tədbirlərini təkmilləşdirmək üçün istifadə edilə bilər. Bu, təşkilata təhlükəsizlik sistemini daim təkmilləşdirməyə imkan verir.

Beləliklə, müdaxilənin aşkarlanması sistemlərinin əsas məqsədi kibertəhlükələrin monitorinqi, müəyyən edilməsi, təhlili və cavab tədbirləri vasitəsilə informasiya sistemlərinin təhlükəsizliyini təmin etməkdir.

Müdaxilənin qarşısının alınması sistemləri (Intrusion Prevention Systems) real vaxt rejimində kiberhücumları aktiv şəkildə aşkar etmək və qarşısını almaq üçün nəzərdə tutulmuşdur. IPS nəinki şübhəli fəaliyyəti aşkarlayır, həm də avtomatik olaraq onu bloklamaq üçün tədbirlər görür, potensial təhdidlər zərər vurmazdan əvvəl qarşısını alır. IPS-in əsas komponentlərinə daxildir:

- Trafik monitorinqi və təhlili.
- Avtomatik cavablandırma.
- İmzalardan və evristik analizdən istifadə.
- Digər təhlükəsizlik sistemləri ilə inteqrasiya.
- Qeydiyyat və hesabat.

Trafik monitorinqi və təhlili – IPS davamlı olaraq şəbəkə trafikinə nəzarət edir və müdaxilə əlamətlərini müəyyən etmək üçün onu təhlil edir. Bu proses məlumat paketlərinin və onların məzmununun dərin təhlilini əhatə edir.

Avtomatik cavablandırma – IDS-dən fərqli olaraq, IPS real vaxt rejimində hücumları dayandıraraq şübhəli trafiki avtomatik bloklaya və ya rədd edə bilər. Bu, müxtəlif təhlükəsizlik siyasətləri və filtrləmə qaydalarının tətbiqi ilə əldə edilir.

İmzalardan və evristik analizdən istifadə – IPS yeni və naməlum hücumları müəyyən etmək üçün məlum təhdidlərin imza verilənlər bazalarından, eləcə də evristik analiz üsullarından istifadə edir. Bu, sistemə geniş spektrli təhdidlərə cavab verməyə imkan verir.

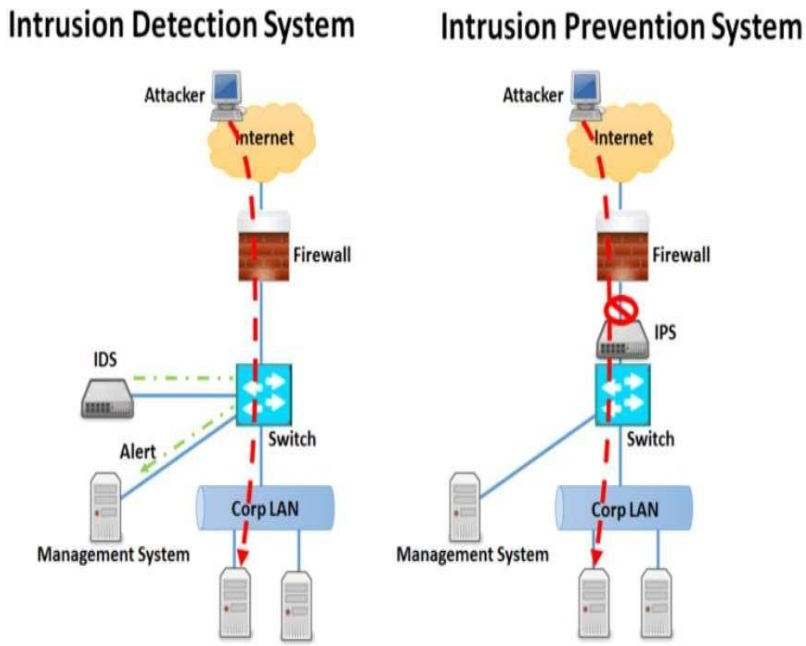
Digər təhlükəsizlik sistemləri ilə inteqrasiya – Ümumi təhlükəsizlik effektivliyini artırmaq üçün IPS tez-tez firewall və təhlükəsizlik hadisələrinin idarə edilməsi (SIEM) sistemləri kimi digər təhlükəsizlik sistemləri ilə inteqrasiya olunur.

Qeydiyyat və hesabat – Bütün sistem hərəkətləri jurnallarda və hesabatlarda qeyd olunur ki, bu da inzibatçılara insidentləri təhlil etməyə və görülən tədbirlərin effektivliyini qiymətləndirməyə imkan verir.

IPS-in əsas funksiyalarına daxildir:

- Real vaxtda hücumun qarşısının alınması.
- Məlum və yeni təhlükələrdən qorunma.
- Məlumatların tamlığını və məxfiliyinin qorunması.
- Hücumların nəticələrini minimuma endirilməsi.
- Normativ tələblərə uyğunluğun təmin edilməsi

IPS-in əsas məqsədi təhdidləri dərhal bloklamaq, müdaxilə edənlərin daxil olmasının qarşısını almaq və mümkün zərəri minimuma endirməkdir. Bu, təşkilata yüksək səviyyədə təhlükəsizlik və əməliyyat sabitliyini saxlamağa imkan verir. IPS, məlum hücumlar və yeni, əvvəllər məlum olmayan zəifliklər də daxil olmaqla geniş spektrli təhlükələrdən qoruyur. İmza və evristik təhlilin birləşməsi sayəsində sistemlər hətta mürəkkəb təhdidləri müəyyən edə və zərərsizləşdirə bilir. İcazəsiz giriş və hücumların qarşısını alaraq, IPS təşkilatın kritik məlumatlarının bütövlüyünü və məxfiliyini qorumağa kömək edir. Təhdidlərə sürətli reaksiya sistemin dayanma müddətini əhəmiyyətli dərəcədə azalda və əhəmiyyətli maliyyə itkilərinin qarşısını ala bilər. Bu, biznesin davamlılığının təmin edilməsinin vacib olduğu təşkilatlar üçün xüsusilə vacibdir (şəkil 10.1).



Şəkil 10.1. IDS və IPS sistemləri

IPS təşkilatlara GDPR, PCI DSS və digərləri kimi kibertəhlükəsizlik qaydalarına və standartlarına riayət etməyə kömək edir. Bu, tənzimlənən sənaye sahələrində fəaliyyət göstərən təşkilatlar üçün xüsusilə vacibdir.

Beləliklə, müdaxilənin qarşısının alınması sistemlərinin əsas məqsədi kibertəhlükələrin aşkarlanması, təhlili və dərhal bloklanması yolu ilə informasiya sistemlərini aktiv şəkildə qorumaqdır. Bu, bizə kiberhücumlarla bağlı riskləri minimuma endirməyə və informasiya infrastrukturunun yüksək səviyyədə təhlükəsizliyini təmin etməyə imkan verir. Çox vaxt IDS və IPS sistemləri şəbəkə təhlükəsizliyinin daha tam səviyyəsini təmin etmək üçün birlikdə istifadə olunur

MAS (IDS) İŞLƏMƏ MEXANİZMİ VƏ NÖVLƏRİ

Hücumun aşkarlanması sistemi (IDS) mümkün müdaxilə və ya təhlükəsizlik pozuntusunu göstərə bilən anomal və ya şübhəli nümunələri aşkar etmək üçün xüsusi hostlarda şəbəkə trafikini və ya fəaliyyətini davamlı olaraq izləməklə işləyir. Hücumun aşkarlanması sistemlərinin işləmə mexanizmi aşağıdakı ardıcıllıqla fəaliyyət göstərir:

- Trafik monitorinqi.
- Məlumatların toplanması və təhlili.
- Analiz üsulları.
- Xəbərdarlığın yaradılması.
- Qeydiyyat və hesabat.

IDS real vaxt rejimində şəbəkə trafikinə və ya hostlardakı hadisələrə nəzarət edir. Şəbəkə səviyyəli sistemlər (NIDS) şəbəkədən keçən məlumatları təhlil edir, ana səviyyəli sistemlər (HIDS) isə fərdi cihazlarda baş verən hadisələri izləyir. Toplanmış məlumatlara şəbəkə paketləri, sistem qeydləri, proqram qeydləri və şəbəkə və ya hostlarda fəaliyyətlə bağlı digər məlumatlar daxildir. IDS məlum hücum imzaları olan verilənlər bazalarından istifadə edir. İmzalardan birinə uyğun gələn trafik aşkar edildikdə, xəbərdarlıq yaradılır. IDS normal sistem davranışı modellərini qurur və hücumları göstərə biləcək bu modellərdən kənarlaşmaları müəyyən edir. Dəqiqliyi artırmaq və yanlış pozitivləri azaltmaq üçün imza və anomal analizi birləşdirir.

Şübhəli fəaliyyət aşkar edildikdə, IDS sistem administratorları üçün mümkün təhlükələri göstərən və onlara tez cavab verməyə imkan verən

xəbərdarlıqlar yaradır. Bütün aşkar edilmiş hadisələr jurnallarda qeyd olunur, sonrakı təhlil və təhlükəsizliyin yaxşılaşdırılması üçün tədbirlər görülməsi üçün hesabatlar yaradılır.

- Hücum aşkarlama sistemlərinin aşağıdakı növləri mövcuddur:
- Şəbəkəyə müdaxilənin aşkarlanması sistemləri (NIDS);
- Host Intrusion Detection Systems (HIDS);
- İmza əsaslı hücum aşkarlama sistemləri;
- Anomaliya əsaslı hücum aşkarlama sistemləri;
- Hibrid hücum aşkarlama sistemləri;
- Şəbəkəyə müdaxilənin aşkarlanması sistemləri (NIDS);
- Proqram təminatı və aparat IDS.

NIDS paket səviyyəsində məlumatları təhlil edərək bütün şəbəkənin və ya onun seqmentlərinin trafikinə nəzarət edir. Nümunə olaraq Snort, Bro (Zeek) göstərmək olar. NIDS-in üstünlüyü son cihaz konfiqurasiyalarında dəyişiklik tələb etmədən real vaxt rejimində hücumları aşkar etmək imkanı malikdir.

Host Intrusion Detection Systems (HIDS) fərdi hostlarda quraşdırılır və sistem qeydlərini, fayl sistemini, proqram qeydlərini və xüsusi cihazdakı fəaliyyətlə bağlı digər məlumatları təhlil edir. Nümunə olaraq OSSEC, Tripwire göstərmək olar. HIDS-in üstünlüyü daxildən edilən hücumlar da daxil olmaqla, birbaşa xüsusi cihazlara yönəlmiş hücumları aşkar edə bilir.

İmza əsaslı hücum aşkarlama sistemləri təhlükələri müəyyən etmək üçün məlum hücum imzalarının verilənlər bazasından istifadə edir. Məlum hücumların aşkarlanmasında yüksək dəqiqlik göstərir.

Anomaliya əsaslı hücum aşkarlama sistemləri normal davranış modellərini qurur və onlardan kənarlaşmaları aşkar edir. Yeni, əvvəllər naməlum hücumları aşkar edə bilir.

Hibrid hücum aşkarlama sistemləri aşkarlamanın effektivliyini artırmaq üçün imza və anomal analiz üsullarını birləşdirir. Əvvəlki hər iki üsulun üstünlüklərini birləşdirir, daha geniş təhlükə əhatəsini təmin edir və yalan pozitivləri azaldır.

Proqram təminatı və aparat İDS Mövcud aparatda proqram təminatı kimi quraşdırılır. Nümunə olaraq Snort, OSSEC göstərmək olar. Bunlar yalnız IDS funksiyalarını yerinə yetirmək üçün nəzərdə tutulmuş ayrı cihazlardır. Nümunə olaraq Cisco, Juniper-dən xüsusi cihazlar. Aiddir.

Müdaxilənin aşkarlanması sistemləri kibertəhlükəsizliyin mühüm elementidir, şəbəkədə və ya hostlarda şübhəli fəaliyyətin vaxtında aşkar edilməsini və bildirişini təmin edir. IDS növlərinin və iş üsullarının müxtəlifliyi

təşkilatlara informasiya sistemlərini geniş spektrli təhlükələrdən qorumaq üçün ən uyğun həll yollarını seçməyə imkan verir.

24/7 monitorinq – IDS heç vaxt yatmır, daim nəzarət edir

Erkən təhlükənin aşkarlanması – Böyük zərər baş verməzdən əvvəl hadisələri müəyyən edir

Kompleks giriş – Təhlil üçün dəyərli məhkəmə məlumatları təqdim edir

Bildiriş xəbərdarlıqları – Potensial pozuntular barədə dərhal adminləri xəbərdar edir

Uyğunluq dəstəyi – Tənzimləyici tələblərə cavab verməyə kömək edir.

MQS (IPS) İŞLƏMƏ MEXANİZMİ VƏ NÖVLƏRİ

Müdaxilənin qarşısının alınması sistemləri (Intrusion Prevention Systems, IPS) aşağıdakı mexanizmə uyğun fəaliyyət göstərir:

- Trafik monitorinqi.
- Məlumatların təhlili.
- Avtomatik cavablandırma.
- Qeydiyyat və hesabatlılıq.
- Digər təhlükəsizlik sistemləri ilə inteqrasiya.

MQS davamlı olaraq real vaxt rejimində şəbəkə trafikinə nəzarət edir. Onlar şəbəkədən keçən məlumat paketlərini təhlil edir, həmçinin fərdi cihazlarda sistem və proqram qeydlərini təhlil edə bilirlər. MQS məlum hücumların imzalarının verilənlər bazasından istifadə edir. İmzalardan birinə uyğun gələn trafik aşkar edilərsə, sistem onu bloklaya bilər. MQS normal sistem davranışı modellərini yaradır və hücumları göstərə biləcək anomaliyaları müəyyən edir. MQS protokol pozuntularını və şübhəli fəaliyyəti müəyyən edərək şəbəkə əlaqələrinin vəziyyətini və kontekstini izləyir. Şübhəli fəaliyyət aşkar edildikdə, MQS avtomatik olaraq trafikin bloklanması, bağlantıların sıfırlanması, firewall qaydalarının dəyişdirilməsi və administratorlara xəbərdarlıq kimi tədbirlər görə bilər. Bütün IPS hərəkətləri jurnallarda qeyd olunur, sistemin effektivliyinin sonrakı təhlili və qiymətləndirilməsi üçün hesabatlar yaradılır. MQS hərtərəfli təhlükəsizliyi əhatə etmək üçün firewall, təhlükəsizlik hadisələrinin idarə edilməsi sistemləri (SIEM), antivirus proqramı və digər təhlükəsizlik alətləri ilə inteqrasiya edə bilər.

Müdaxilənin qarşısının alınması sistemlərinin (MQS) əsas növlərinə aşağıdakılar daxildir:

- Şəbəkə Hücumlarının Qarşısının Alınması Sistemləri (NIPS).
- Host əsaslı hücumların qarşısının alınması sistemləri (HIPS).
- İmza əsaslı hücumun qarşısının alınması sistemləri.
- Anomaliya əsaslı hücumların qarşısının alınması sistemləri.
- Proqram təminatı və aparat IPS.

Şəbəkə hücumlarının qarşısının alınması sistemləri (NIPS) – şəbəkə səviyyəsində hücumları müəyyən etmək və qarşısını almaq üçün bütün şəbəkə və ya onun seqmentləri üzrə trafikə nəzarət edir və təhlil edir. Nümunə olaraq Cisco Firepower, Palo Alto Networks göstərmək olar. NIPS-in üstünlüyü Hücumları real vaxtda bloklamaq, bütün şəbəkəni qorumaqdır.

Host əsaslı hücumların qarşısının alınması sistemləri (HIPS) – fərdi hostlarda quraşdırılır və sistem qeydlərini, fayl sistemini və proqram qeydlərini təhlil edir. Nümunə olaraq Symantec Endpoint Protection, McAfee Host Intrusion Prevention göstərmək olar. NIPS-in üstünlüyü Xüsusi cihazları, o cümlədən serverləri və iş stansiyalarını yerli hücumlardan və təhdidlərdən qorumaqdır.

İmza əsaslı hücumun qarşısının alınması sistemləri – təhlükələrin qarşısını almaq üçün məlum hücum imzalarının verilənlər bazalarından istifadə edir. Bu sistemin üstünlüyü məlum hücumların aşkarlanması və bloklanmasında yüksək dəqiqlik, az sayda yanlış pozitivlik təqdim etməkdir.

Anomaliya əsaslı hücumların qarşısının alınması sistemləri normal davranış nümunələri yaradır və hücumları göstərə biləcək kənarlaşmaları bloklayır. Bu sistemin üstünlüyü yeni, əvvəllər naməlum hücumları aşkarlaya və qarşısını ala bilir.

Hibrid hücumların qarşısının alınması sistemləri – səmərəliliyi artırmaq üçün imza və anormal analiz üsullarını birləşdirir. Bu sistemin üstünlüyü hər iki üsulun üstünlüklərini birləşdirir, daha geniş təhlükə əhatəsini təmin edir və yalan pozitivləri azaldır.

Proqram təminatı və aparat IPS – proqram IPS mövcud aparatda proqram təminatı kimi quraşdırılır. Hardware IPS yalnız IPS funksiyalarını yerinə yetirmək üçün nəzərdə tutulmuş ayrı cihazlardır.

Hücumların qarşısının alınması sistemləri hərtərəfli kibertəhlükəsizlik strategiyasının mühüm tərkib hissəsidir. Onların real vaxt rejimində hücumları nəinki aşkar etmək, həm də qarşısını almaq qabiliyyəti onları şəbəkələri və sistemləri geniş spektrli kibertəhlükələrdən qorumaq üçün əvəzolunmaz edir.

IPS növlərinin müxtəlifliyi təşkilatınızın xüsusi ehtiyacları və infrastrukturu üçün ən uyğun həlləri seçməyə imkan verir.

MAS (IDS) ilə MQS (İPS) ARASINDAKI FƏRQ

Hücumun aşkarlanması sistemləri (IDS) və müdaxilənin qarşısının alınması sistemləri (IPS) hər ikisi şəbəkə təhlükəsizliyini təmin etmək üçün nəzərdə tutulmuşdur, lakin funksionallığa, təhdidlərə cavab və avtomatlaşdırma səviyyəsinə görə bir neçə əsas fərqə malikdir (cədvəl 10.1). Cədvəldən göründüyü kimi sistem müxtəlif paramterlərə görə fərqləndirilir:

Cədvəl 10.1.

Parametr	**Hücumun aşkarlanması sistemi (IDS)**	**Hücumun qarşısının alınması sistemi (IPS)**
Əsas funksiyası	Aşkarlama və Xəbərdarlıq	Qarşısının alınması və bloklanması
Cavab mexanizmi	Təhlükəsizlik işçiləri üçün xəbərdarlıqlar yaradır	Şübhəli trafiki aktiv şəkildə bloklayır və ya pozur
Fokus nöqtəsi	Potensial təhlükələrin müəyyən edilməsi	Təhdidlərin şəbəkənizə çatmasının qarşısının alınması
Şəbəkə performansına təsir	Təsiri azaldın, çünki o, yalnız trafikə nəzarət edir	Potensial olaraq daha yüksək təsir, çünki düzgün konfiqurasiya edilmədikdə qanuni trafiki (yanlış pozitivlər) bloklaya bilər.
Yerləşdirmə strategiyası	Daha çevik, şəbəkə əsaslı və ya host əsaslı konfiqurasiyalarda yerləşdirilə bilər	Tez-tez daha sürətli cavab verməк üçün şəbəkə axını daxilində in-line yerləşdirilir

Xərc	Ümumiyyətlə, IPS-dən daha ucuzdur	Real vaxt analizi və bloklama imkanlarının mürəkkəbliyinə görə daha bahalı ola bilər
Sıfır gün Hücumları üçün uyğunluq	Tamamilə yeni hücumlara qarşı məhdud effektivlik	Xüsusi hücum imzası naməlum olsa belə, şübhəli fəaliyyəti bloklamaqla hələ də bəzi qoruma təklif edə bilər
Həyəcan xəbərdarlığı	Effektiv filtrləmə və prioritetləşdirmə tələb edən yüksək həcmli xəbərdarlıqlar yarada bilər	Xəbərdarlıq yaratmaq ehtimalı azdır, konfiqurasiya təhdidlərə səbəb ola bilər.

Funksionallığa görə İDS/İPS arasındakı fərq:

- IDS yalnız şəbəkədəki potensial təhlükələri və anomaliyaları aşkar etmək üçün nəzərdə tutulmuşdur. Onlar hücumları, virusları, müdaxilələri və digər potensial təhlükəsizlik problemlərini müəyyən etmək üçün şəbəkə trafikini və ya hostlardakı fəaliyyəti təhlil edə bilərlər.

-IPS IDS-dən fərqli olaraq, IPS nəinki təhdidləri aşkar edir, həm də onların şəbəkəyə təsirini aktiv şəkildə qarşısını alır və ya minimuma endirir. Onlar potensial zərərli fəaliyyətləri və ya əlaqələri avtomatik bloklaya, məhdudlaşdıra və ya dayandıra bilər.

Təhdidlərə cavaba görə İDS/İPS arasındakı fərq:

- IDS aşkar edilmiş təhlükələr haqqında məlumat verir, lakin hücumların qarşısını almaq və ya qarşısını almaq üçün aktiv addımlar atmır. Onlar administratoru mümkün problemlər barədə xəbərdar edir, bundan sonra administrator təhlükəyə cavab vermək üçün tədbir görməlidir.

- IPS şübhəli resurslara və ya əlaqələrə girişi bloklamaq, cihazları və ya proqramları söndürmək, hücum paketlərini bloklamaq və s. vasitəsilə aşkar edilmiş təhdidlərə avtomatik cavab verməyə qadirdir.

Avtomatlaşdırma səviyyəsinə görə İDS/İPS arasındakı fərq:

- IDS aşkar edilmiş təhlükələri təhlil etmək və onlara cavab vermək üçün tədbirlər görmək üçün insan müdaxiləsini tələb edir. Onlar idarəçilərə şəbəkə təhlükəsizliyi ilə bağlı qərarlar qəbul etmək üçün məlumat verirlər.

- IPS inzibatçının müdaxiləsinə ehtiyac olmadan təhdidləri bloklamaq və ya qarşısını almaq üçün tədbirlər görərək avtomatik hərəkət edə bilər. Bu, təhdidlərə daha tez və effektiv cavab verməyə imkan verir.

Beləliklə, IDS və IPS arasındakı əsas fərq onların aşkar edilmiş təhdidlərə cavab vermək qabiliyyətidir: IDS yalnız təhdidləri aşkar edir və idarəçiləri məlumatlandırır, IPS isə təhlükəsizlik təhdidlərinin qarşısını almaq və ya bloklamaq üçün aktiv tədbirlər görür.

SIEM - HADİSƏ VƏ MƏLUMATLARIN TƏHLÜKƏSİZ İDARƏETMƏ SİSTEMLƏRİ

SIEM (Security Information and Event Management) sistemləri təşkilatın informasiya sistemlərinin və şəbəkələrinin təhlükəsizliyini təmin etmək üçün nəzərdə tutulmuşdur. SIEM sistemlərinin əsas məqsədi təhlükəsizlik divarları, müdaxilənin aşkarlanması sistemləri, serverlər, proqramlar və şəbəkə cihazları kimi müxtəlif mənbələrdən qeydləri və hadisələri toplayır. Anomaliyaları və potensial təhlükələri müəyyən etmək üçün toplanmış məlumatları təhlil edir. Hadisə korrelyasiyası fərdi insidentləri əlaqələndirməyə və mürəkkəb hücumları müəyyən etməyə imkan verir. Real vaxt rejimində təhlükəsizlik monitorinqini və şübhəli fəaliyyət və ya anomaliyalar barədə xəbərdarlıqları təmin edir. Bu, təhdidlərə tez cavab verməyə imkan verir. Ətraflı qeydlər və hadisələr zəncirini yenidən qurmaq imkanı təmin etməklə təhlükəsizlik insidentlərini təhlil etməyə və araşdırmağa kömək edir. Qeydlərin toplanması və saxlanmasını avtomatlaşdırmaqla müxtəlif təhlükəsizlik standartları və qaydalarına (məsələn, GDPR, HIPAA, PCI-DSS) uyğunluğu təmin etməyə kömək edir. SIEM-in işləmə mexanizmi aşağıdakı mərhələlərdən ibarətdir:

- Məlumatların toplanması.
- Məlumatların birləşdirilməsi.
- Təhlil və korrelyasiya.
- Monitorinq və xəbərdarlıq.
- Hesabat və vizuallaşdırma.

SIEM sistemi real vaxt rejimində müxtəlif mənbələrdən məlumatları toplayır. Bunlar şəbəkə cihazları, serverlər, proqramlar, verilənlər bazası və

digər infrastruktur elementləri ola bilər. Toplanmış məlumatlar sonrakı təhlili asanlaşdırmaq üçün toplanır və normallaşdırılır. Normallaşdırma məlumatların vahid formata gətirilməsini nəzərdə tutur. SIEM sistemi anomaliyaları və potensial təhlükələri müəyyən etmək üçün korrelyasiya qaydaları, maşın öyrənməsi və digər üsullardan istifadə edərək məlumatları təhlil edir. Şübhəli fəaliyyət və ya təhlükə aşkar edilərsə, sistem təhlükəsizlik operatorları üçün xəbərdarlıqlar və bildirişlər yaradır. SIEM asan təhlil və qərar qəbul etmək üçün hesabat və məlumatların vizuallaşdırılmasını təmin edir. Buraya tablolar, qrafiklər və cədvəllər daxil ola bilər.

SIEM işləmə rejimlərinə daxildir:

1. Real vaxt – Məlumatların işlənməsi və təhlili real vaxt rejimində baş verir ki, bu da təhlükəsizlik insidentlərinə tez reaksiya verməyə imkan verir.

2.Qayda əsaslı təhlil – SIEM anomaliyaları və təhlükələri müəyyən etmək üçün əvvəlcədən konfiqurasiya edilmiş korrelyasiya qaydalarından istifadə edir. Bu qaydalar əl ilə və ya avtomatlaşdırılmış şəkildə konfiqurasiya edilə bilər.

3. Maşın öyrənməsi – Müasir SIEM sistemləri davranış nümunələri və anomaliyaları təhlil edərək yeni və naməlum təhlükələri müəyyən etmək üçün maşın öyrənmə alqoritmlərindən istifadə edir.

4. Tarixi təhlil – SIEM tendensiyaları müəyyən etmək, keçmişdə baş vermiş hadisələri araşdırmaq və korrelyasiya qaydalarını təkmilləşdirmək üçün tarixi məlumatları təhlil etməyə imkan verir.

5. Avtomatlaşdırma – Bəzi SIEM sistemləri insidentlərə cavab verməni avtomatlaşdırmaq üçün digər təhlükəsizlik alətləri ilə inteqrasiya edir ki, bu da təhdidlərin aşkarlanması və onlara cavab verilməsi prosesini sürətləndirir.

SIEM sistemləri müəyyən etmək, təhlil etmək və cavab vermək üçün alətlər təqdim etməklə informasiya sistemlərinin təhlükəsizliyinin təmin edilməsində əsas rol oynayır.

Ən məhşur SIEM sistemləri aşağıdakılardır:

- HP ArcSight
- IBM QRadar,
- McAfee ESM,
- Symantec SIM
- Cisco MARS
- GFI ESM.

HP ArcSight - Hewlett-Packard (HP) tərəfindən hazırlanıb və monitorinq, təhlükənin aşkarlanması, məlumat analitikası və hesabat imkanları təklif edir.

Anomaliyaları və təhlükəsizlik təhdidlərini müəyyən etmək üçün müxtəlif mənbələrdən böyük həcmdə məlumatların toplanması və təhlilini dəstəkləyir. Çevik konfiqurasiya seçimlərinə və digər HP təhlükəsizlik məhsulları ilə inteqrasiyaya malikdir.

IBM Qradar - Təhlükəsizlik məlumatlarının toplanması, təhlili və vizuallaşdırılması imkanlarını təmin edən IBM Security məhsuludur. Hadisə korrelyasiyası, anomaliyaların aşkarlanması, hücumların aşkarlanması və insidentlərin idarə edilməsi funksiyalarını təklif edir. Digər təhlükəsizlik məhsulları və bulud xidmətləri ilə geniş inteqrasiya imkanlarına malikdir.

McAfee ESM - McAfee-dən (indi Intel Security-nin bir hissəsi) təhlükəsizlik hadisələrinin idarə edilməsi sistemidir. Şəbəkə və proqram təhlükəsizliyinin toplanması, təhlili, korrelyasiya və hesabat funksiyasını təmin edir. Digər McAfee təhlükəsizlik məhsulları ilə inteqrasiya var.

Symantec SİM kartı - Əvvəllər Symantec Təhlükəsizlik Məlumat Meneceri kimi tanınan o, təhlükəsizlik məlumatlarını toplamaq, təhlil etmək və idarə etmək üçün alətlər təqdim edir. Təhlükənin aşkarlanması, hadisə korrelyasiyası və digər Symantec təhlükəsizlik məhsulları ilə inteqrasiya təklif edir.

Cisco MARS (Cisco Təhlükəsizlik Meneceri)- təhlükəsizlik hadisələrinin toplanması, təhlili və hesabatı daxil olmaqla, təhlükəsizliyin idarə edilməsi imkanlarını təmin edir. Cisco ASA (Adaptive Security Appliance) və digər cihazlar kimi Cisco təhlükəsizlik məhsulları ilə inteqrasiyaya malikdir.

GFI ESM - Şəbəkə təhlükəsizliyinin toplanması, təhlili və hesabat vermə funksiyalarını təmin edir. Şəbəkə təhlükəsizliyini təmin etmək üçün hadisələrin monitorinqi, təhlükənin aşkarlanması və insidentlərin idarə edilməsi imkanlarını təmin edir.

Bu sistemlərin hər birinin öz xüsusiyyətləri, üstünlükləri və məhdudiyyətləri var və xüsusi SIEM platformasının seçimi təşkilatın unikal tələb və ehtiyaclarından asılıdır.

TƏHLÜKƏSİZLİK ƏMƏLİYYATLARI MƏRKƏZİ (SOC)

Təhlükəsizlik əməliyyatları mərkəzi (Security Operating Center) sözün həqiqi mənasında operativ təhlükəsizlik mərkəzidir. Fəaliyyətinin əsas məqsədi informasiya təhlükəsizliyi insidentlərini müəyyən etmək və onlara

reaksiya verməkdir. SOC-a əlavə olaraq, praktikada tez-tez sinonim kimi qəbul edilən digər abbreviaturalar da var:

CERT (Computer Emergency Response Team) – kompüter təcili yardım qrupu;

CSIRT (Computer Security Incident Response Team) kompüter təhlükəsizliyi ilə bağlı insidentlərə cavab verən qrupdur.

Təcrübədə bu strukturlar hadisələrin müəyyən edilməsi, cavablandırılması və araşdırılması ilə bağlı mahiyyətcə eyni vəzifələri yerinə yetirsələr də, hələ də bəzi fərqlərə malikdirlər. Beləliklə, CERT-lər müəyyən bir sahəyə yönəldilir, məsələn, FinCERT (kredit və maliyyə sektoru), GovCERT (əvvəlcə dövlətin informasiya resursları sferasına yönəldilib, daha sonra ona kritik informasiya infrastrukturu ilə bağlı sahələr əlavə edildi), cari təhlükələrin monitorinqi üçün CSIRT-lər , hadisələrin məlumat bazasının yaradılması və iştirakçılar arasında məlumat mübadiləsi, məsələn, CSIRT-RU (müxtəlif mülkiyyət formalı təşkilatların informasiya təhlükəsizliyi xidmətləri arasında insidentlər haqqında məlumat mübadiləsi üçün yaradılmışdır). Əksər hallarda CERT/CSIRT bir növ SOC assosiasiyalarıdır.

Hazırda yaradılmış kompüter hücumlarının aşkarlanması, qarşısının alınması və nəticələrinin aradan qaldırılması üzrə dövlət sistemi (GosSOPKA) əslində həm də müxtəlif SOC-ları (departament (korporativ) mərkəzləri (seqmentlər)) birləşdirən CERT-ni təmsil edir.

SOC Funksiyaları və prosesləri. SOC-un struktur sxemi şəkil 10.2-də təsvir olunmuşdur.

Şəkil 10.2. SOC-un strukturu

Diaqramdan göründüyü kimi, SOC daxilində əsas proseslər hadisələrin emalı ilə bağlıdır. Hadisənin idarə edilməsi prosesinə daha ətraflı baxaq.

Hadisənin aşkarlanması və qeydiyyatı. İnformasiya təhlükəsizliyi təhdidlərinin yaranmasına səbəb olan amilləri və onların həyata keçirilməsini vaxtında müəyyən etmək üçün informasiya təhlükəsizliyi tələblərinə əməl olunmasına daxili nəzarət həyata keçirilir ("hazırlıq" adlanır), bu zaman informasiya təhlükəsizliyi insidentləri müəyyən edilə bilər. İnformasiya resursları daim nəzarətdə saxlanılır. Hadisələr haqqında məlumat mənbələrinə audit jurnalları, iş stansiyalarının məzmunu (onlarda saxlanılan fayllar), şəbəkə trafiki, SIEM və DLP sistemlərinin qeydləri, instrumental monitorinq məlumatları və istifadəçi sorğuları (şikayətlər) daxildir.

Hadisənin aşkarlanması. İnformasiya təhlükəsizliyinə təhlükənin baş verdiyini, həyata keçirildiyini və ya baş verməsi ehtimalını göstərən hadisə aşkar edilərsə, o, qeydə alınır.

Hadisəyə/hadisəyə operativ reaksiya. İnformasiya təhlükəsizliyi təhdidinin ehtimal olunan həyata keçirilməsini göstərən hadisə baş verdikdə (insident göstəricisi) ehtimal olunan təhlükə mənbəyi lokallaşdırılır.

Hadisəyə cavab. Hadisənin baş verdiyi bəlli olduqdan sonra istintaqın sənədləşdirilməsinə və sübutların toplanmasına başlanılır. Onun zərərsizləşdirilməsi üçün strategiya və prosedurlar müəyyən edilir, müvafiq amillər əsasında hadisənin idarə edilməsi üçün prioritetlər müəyyən edilir və müvafiq şəxslərə məlumat verilir.

Hadisənin araşdırılması. Hadisənin bütün səbəbləri müəyyən edilənə qədər hadisənin araşdırılması davam etdirilir. Hadisənin təhqiqat prosesində iştirak edən işçilər hücumu (uğursuzluğu) başlatmış şəxslər, bu şəxslərin hərəkətlərinin ardıcıllığı, hücumun motivləri, sövdələşmənin mövcudluğu və cinayətin müəyyən edilməsinə kömək edən digər məlumatlar haqqında mümkün qədər çox məlumat toplamalıdırlar. Lazım gələrsə, xarici resurslarla - digər SOC\CERT\CSIRT, insidentlərin araşdırılması sahəsində təcrübəsi olan podratçılarla qarşılıqlı əlaqə (kömək sorğusu) həyata keçirilir. SOC-un inkişaf səviyyələri cədvəl 10.2-də göstərildiyi kimi qruplaşdırılmışdır.

Prosesləri təkmilləşdirmək üçün PDCA dövrü (Deming Cycle) istifadə olunur: P – Plan, D – Et, C – Nəzarət, A – Akt. İdarəetmə sistemlərində, o cümlədən informasiya təhlükəsizliyində istifadə olunan klassik dövr hesab olunur.

Cədvəl 10.2.

Səviyyə	İnkişaf səviyyəsinin təyini	İnkişaf səviyyəsinin təsviri
0	Yarımçıq proses	Belə bir proses hələ həyata keçirilməyib və ya məqsədə uyğun deyil. Məsələn, əsas SOC prosesləri yoxdur
1	Həyata keçirilən proses	Tamamlanmış proses öz məqsədinə çatdı. Məsələn, informasiya təhlükə-sizliyi insidentlərinin idarə edilməsi prosesi həyata keçirilir, lakin sənədləşdirilmir
2	İdarə olunan proses	Proses nəzarət olunan şəkildə həyata keçirilir (planlaşdırılır, nəzarət edilir və monitorinq edilir) və onun iş məhsulları müvafiq qaydada qurulur, nəzarət edilir və saxlanılır. Məsələn, informasiya təhlükəsizliyi insidentləri üçün ölçülər var
3	Qurulmuş proses	Bu səviyyədə idarə olunan proses həmin prosesin nəticələrinə nail olmaq iqtidarında olan müəyyən edilmiş prosesdən istifadə etməklə həyata keçirilir. Məsələn, informasiya təhlükəsizliyi insidentlərinin emalı üçün sənədləşdirilmiş bir proses var, insident göstəriciləri sənədləşdirilir.
4	Proqnozlaşdırıla bilən proses	Bu səviyyədəki proses bu prosesin nəticələrinə nail olmaq üçün müəyyən sərhədlər daxilində həyata keçirilir. Məsələn, insidentlərin aşkarlanması və

		idarə olunması hədəfləri sənədləşdirilir və yerinə yetirilir.
5	Optimallaşdırma prosesi	Bu səviyyədə proqnozlaşdırıla bilən proses müvafiq cari və planlaşdırılan biznes məqsədlərinə nail olmaq üçün davamlı olaraq təkmilləşdirilir. Məsələn, SOC-un səmərəliliyinin müntəzəm olaraq qiymətləndirilməsi aparılır, maksimum əsas fəaliyyət göstəricilərinə nail olmaq üçün proseslər qurulur.

SOC yaradılması prosesinin xüsusiyyətləri. SOC-nun yaradılması bir növ layihə kimi qəbul edilə bilər və müvafiq olaraq, onun yaradılması üçün layihənin idarə edilməsi proseslərindən istifadə edilə bilər. Şərti olaraq, SOC yaratmaq layihəsini müxtəlif mərhələlər daxil olmaqla üç mərhələyə bölmək olar. Layihənin ilkin mərhələsi bu mərhələdə SOC-in layihələndirilməsi olacaq, mərkəzə olan tələblər müəyyən edilir (texniki tapşırıqlar hazırlanır), texniki infrastruktur layihələndirilir (texniki layihə hazırlanır) və layihə; komanda formalaşır.

İkinci mərhələ, hazırlanmış texniki layihəyə uyğun olaraq SOC-un texniki infrastrukturunun yaradılması və texniki infrastrukturun istismara verilməsi, yəni. mahiyyətcə SOC-un texniki təchizatı. Eyni zamanda, istismara verildikdən sonra informasiya təhlükəsizliyi ilə bağlı insidentlərin monitorinqi və cavab tədbirləri sistemli olmayacaq.

Üçüncü mərhələ SOC-un özünün işləməsi və proseslərin təkmilləşdirilməsi (onların yetkinlik səviyyəsinin yüksəldilməsi) ilə bağlıdır: monitorinq və reaksiya prosesləri daha rəsmiləşir, əlavə vasitələr meydana çıxır, insidentlərin qarşısının alınması prosesləri qurulur. Daha da inkişaf etdikcə avtomatlaşdırma vasitələrinin çeşidi genişlənir, təcrübə və səriştələrin toplanması təmin edilir, müxtəlif nəzarət ölçüləri hazırlanır, SOC böyüyür və təkmilləşir, informasiya təhlükəsizliyi fəaliyyətlərinin səmərəliliyini əhəmiyyətli dərəcədə artıra bilən alətə çevrilir.

YOXLAMA SUALLARI

1. IDS/IPS sistemləri nədir və onların şəbəkə təhlükəsizliyində rolu nədir?
2. IDS sistemlərinin iş mexanizmi nədir və hansı növ IDS sistemləri mövcuddur?
3. IPS sistemləri necə işləyir və şəbəkələri qorumaq üçün hansı növ IPS sistemlərindən istifadə olunur?
4. IDS və IPS sistemləri arasındakı fərq nədir və bu sistemlər hansı funksiyaları yerinə yetirir?
5. SIEM nədir və onun şəbəkə təhlükəsizliyində IDS/IPS sistemləri ilə necə əlaqəsi var?
6. IDS/IPS sistemləri kontekstində şəbəkə təhlükəsizliyi əməliyyatları mərkəzinin (SOC) rolu nədir?
7. IDS hansı hadisələri aşkar edə bilər və bu şəbəkə təhlükəsizliyinə necə təsir edir?
8. IPS sistemlərinin IDS sistemləri ilə müqayisədə üstünlükləri və çatışmazlıqları nələrdir?
9. IDS/IPS sistemləri tərəfindən hansı növ hücumlar aşkar edilə və qarşısını ala bilər?
10. IDS/IPS sistemləri daxili və xarici şəbəkə təhlükəsizliyi təhdidlərindən qorunmağa necə kömək edə bilər?
11. IDS/IPS sistemlərinin effektiv işləməsini təmin etmək üçün hansı təhlükəsizlik tədbirləri həyata keçirilə bilər?
12. IDS/IPS sistemlərini digər şəbəkə infrastrukturu komponentləri ilə inteqrasiya etmək üçün hansı texnologiyalardan istifadə olunur?
13. IDS/IPS sistemləri şəbəkə performansına necə təsir edə bilər və bu, yerləşdirilərkən necə nəzərə alınır?
14. IDS/IPS sistemləri tərəfindən aşkar edilən hadisələr necə təhlil edilir və təhdidlərə cavab verməkk üçün hansı tədbirlər görülür?
15. IDS/IPS sistemlərini yerləşdirərkən və istifadə edərkən nəzərə alınmalı olan əsas təhlükəsizlik tələbləri hansılardır?

PRAKTİKİ TAPŞIRIQ

1. Antivirus proqramının qurulması və yenilənməsi: Vəzifə viruslardan, troyanlardan və digər zərərli proqramlardan qorunmaq üçün kompüter və cihazlarda antivirus proqramını quraşdırmaq və mütəmadi olaraq yeniləməkdir.

Tapşırıq: Kompüterlərdə və cihazlarda antivirus proqramının müntəzəm olaraq yoxlanılması və yenilənməsi.

Məqsəd: Antivirus proqramının ən son versiyalarını quraşdıraraq və onları mütəmadi olaraq yeniləyərək viruslardan və digər zərərli proqramlardan davamlı müdafiəni təmin etmək.

2. İşçilərə informasiya təhlükəsizliyi qaydaları üzrə təlimlərin keçirilməsi: Təhlükəsizlik qaydaları, o cümlədən etibarsız Wi-Fi şəbəkələrinə qoşulmamaq, mürəkkəb parollardan istifadə zərurəti ilə bağlı işçilər üçün təlim və seminarların keçirilməsi və s.

Tapşırıq: İnformasiya təhlükəsizliyi qaydaları üzrə işçilər üçün təlim və maarifləndirici kursların təşkili.

Məqsəd: Müasir informasiya təhlükəsizliyi təhdidləri barədə işçilərin məlumatlılığını artırmaq və məxfi məlumatların effektiv qorunması üçün onlara lazımi bilik və bacarıqları vermək.

3. Şəbəkə və sistem təhlükəsizliyi auditi: Zəiflikləri, zəif nöqtələri və təcavüzkarlar üçün mümkün giriş nöqtələrini aşkar etmək üçün şəbəkə və sistemlərin müntəzəm auditinin aparılması.

Tapşırıq: Şəbəkə və sistem təhlükəsizliyinin sistemli auditinin aparılması.

Məqsəd: Şəbəkə infrastrukturunda və sistemlərində potensial zəiflikləri və zəiflikləri aşkar etmək, onların aradan qaldırılması və təhlükəsizlik səviyyəsinin yüksəldilməsi üçün tədbirlər görmək.

4. Məlumat Girişinə Nəzarət: Yalnız səlahiyyətli şəxslərin həssas məlumatlara daxil olmasını təmin etmək üçün istifadəçi imtiyazlarını idarə etmək də daxil olmaqla, girişə nəzarət sistemlərini qurun və qoruyun.

Tapşırıq: Məxfi məlumatlara və resurslara girişi idarə etmək.

Məqsəd: Məlumat sızması və icazəsiz giriş riskini minimuma endirməklə, yalnız səlahiyyətli istifadəçilərin həssas məlumatlara çıxış əldə etməsini təmin etmək.

5. Şəbəkə Trafikinə Nəzarət və Anomaliyaların Aşkarlanması: Anormal fəaliyyəti, şübhəli müdaxilə cəhdlərini və digər potensial təhdidləri müəyyən etmək üçün IDS/IPS sistemlərindən istifadə edərək şəbəkə trafikinə müntəzəm olaraq nəzarət edin.

Tapşırıq: Şəbəkə trafikinin monitorinqi və anomaliyaların aşkarlanması.

Məqsəd: Şəbəkəyə hücumları, eləcə də şəbəkənin və məlumatın təhlükəsizliyinə potensial təhlükələri göstərə bilən digər anomaliyaları aşkar etmək və qarşısını almaq.

ƏDƏBİYYAT

16. Azərbaycan Respublikasının Konstitusiyası. Bakı, 2009.
17. Biometrik informasiya haqqında Azərbaycan Respublikasının
18. Qanunu, Bakı, 2008.
19. Dövlət sirrinə aid məlumatların siyahısının ayrılması haqqında Azərbaycan Respublikası Prezidentinin fərmanı. Bakı, 2005.
20. Dövlət sirri haqqında Azərbaycan Respublikasının Qanunu, Bakı, 2004.
21. Azərbaycan haqqında məlumat əldə etmək qanunu, Bakı, 2005.
22. Fərdi məlumatlar haqqında Azərbaycan Respublikasının qanunu, Bakı, 2010.
23. Kommersiya sirri haqqında Azərbaycan Respublikasının qanunu, Bakı, 2001.
24. Azərbaycan Respublikasının məlumat azadlığı haqqında qanunu, Bakı, 1998.
25. Milli təhlükəsizlik haqqında Azərbaycan Respublikasının Qanunu. Bakı, 2004.
26. Məlumat toplularının hüquqi müdafiəsi haqqında Azərbaycan Respublikasının Qanunu, Bakı, 1998. Azərbaycan Respublikası Elm və Təhsil Nazirliyinin "050615 – "İnformasiya təhlükəsizliyi" ixtisası isə 28.07.2022-ci il tarixli F-463 №li əmri ilə təsdiq edilmiş "Bakalavriat səviyyəsinin (əsas (baza) Ali Tibb Təhsilinin)" ixtisas üzrə təhsil proqramı
27. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası, 28 avqust 2023.
28. https://static.president.az/upload/Files/2023/08/29/80f2ffe2545b66274d2eed810cc704d4_5019787.pdf
29. Azərbaycan Respublikası Prezidentinin "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" 2012-ci il 26 sentyabr tarixli 708 nömrəli Fərmanı
30. https://mincom.gov.az/storage/pages/1076/e592f04f37854bc3bf0f35e4fca267e3.pdf
31. Azərbaycan Respublikası Prezidentinin "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanununun icrasının təmin edilməsi barədə" 2010-cu il 13 dekabr tarixli 361 nömrəli Fərmanı
32. https://mincom.gov.az/storage/pages/1085/3679a432d86e41e5637a3f11deec07ea.pdf

33. Azərbaycan Respublikası Prezidentinin “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə” 1998-ci il 19 iyun tarixli 729 nömrəli Fərmanı.
34. https://mincom.gov.az/storage/pages/1127/ac4cd5b4ed930c3a249aec39e8c71e01.pdf
35. İsmayıl Calallı (Sadıqov), “İnformatika terminlərinin izahlı lüğəti”, 2017, “Bakı” nəşriyyatı, 996 s.
36. Əlizadə M.N., Bayramov H.M., Məmmədov Ə.S. İNFORMASİYA TƏHLÜKƏSİZLİYİ, Dərslik, Bakı, “İQTİSAD UNİVERSİTETİ“ nəşriyyatı, şəkilli, 2016 - 384 səh.
37. Həşimov M. Əşyaların İnterneti texnologiyaları əsasında yaradılan şəbəkə mühitində hücumların təhlil // “İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri” IV respublika konfransı, 14 dekabr 2018-ci il, s. 195-198
38. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyat- Poliqrafiya Mərkəzi. 2009, 340 s.
39. Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011, 112 s.
40. Qasımov V.Ə. “İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq”. Bakı, 2007
41. Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011, 112 s.
42. Əliquliyev R. M., İmamverdiyev Y.N. “İnformasiya təhlükəsizliyi insidentləri”. Bakı - 2012, 219 s.
43. Əliquliyev R.M., İmamverdiyev Y.N.. Rəqəm imzası texnologiyası. Бакы: 2003, 130 s.
44. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: 2006, 698 s.
45. Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.
46. Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.

47. Maykl E. Vitman, Herbert C. Mattord. İnformasiya təhlükəsizliyinin prinsipləri (ingilis dilindən tərcümə). Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.
48. Rzayeva G., İbrahimova A. Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi. Dərs vəsaiti. Bakı: "Nurlar" nəşriyyatı, 2021, 200 s.
49. Nieles M., Dempsey K., Pillitteri V.Y., "An Introduction to Information Security", USA, 2017, 101 p.
50. Principles of Information Security, 7th Edition Michael E. Whitman and Herbert J. Mattord
51. Thomas A. Johnson. CYBER Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Webster University St. Louis, Missouri, USA, 2015, p.348
52. Mark Ciampa. CompTIA® Security+ Guide to Network Security Fundamentals, Seventh EditionCengage Learning, Inc. 2022, WCN: 02-300
53. ISO/IEC 14443-1 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. 2000.
54. ISO/IEC 14443-2 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. 2001.
55. Барсуков В.С. Безопасность: технологии, средства, услуги/ В.С.Барсуков. Москва: КУДИЦ-ОБРАЗ, 2001, 496 с.
56. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.Москва: ФОРУМ: ИНФРА-М, 2013. 368 с.
57. Вострецова, Е.В. В78 Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. Екатеринбург: Изд-во Урал. ун-та, 2019.204 с.
58. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с
59. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. Москва: Радио и связь, 2000. 192 с
60. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Москва: Горячая линия — Телеком, 2001. 148 с

61. Келдыш Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. С.100
62. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации: учеб. пособие / Н.В. Келдыш. - М.: Мир науки, 2022. – сетевое издание. Режим доступа: https://izdmn.com/PDF/14ЬТТЗГ22.pdf
63. Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина М.: Национальный Открытый Университет «ИНТУИТ», 2014. 378 с.
64. Олифер В.Г. Безопасность компьютерных сетей. М.: Горячая линия - Телеком, 2018. 644с.
65. Олифер В.Г., Новые технологии и оборудование IP-сетей / В.Г.Олифер, Н.А.Олифер. – СПб.; БХВ-Петербург, 2021. 1005 с.
66. Петров С.В., Петров В.П. Информационная безопасность человека и общества: учебное пособие, 2007.
67. Пушнин А.В. Информационные сети и телекоммуникации / А.В.Пушнин, В.В.Янушко. Таганрог: Изд-во ТРТУ, 2015. 128 с
68. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004.
69. Сарбуков А.у Грушо А. Аутентификация в компьютерных системах // Системы безопасности. 2003. №5(53).
70. Семейство стандартов IEEE 802.11. http://www.wireless.ru/ wireless/wrl_base80211
71. Симонов С. В. Методология анализа рисков в информационных системах // Конфидент. 2001. № 1.
72. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. Издательство Политехнического университета, Санкт-Петербург, 2005.
73. Сизова О.В. Информационная безопасность: учеб. пособие / О.В.Сизова; Иван.гос.хим-технол. ун-т. Иваново, 2015. 120 с.
74. Скородумов Б. Безопасность союза интеллектуальных карточек и персональных компьютеров // Мир карточек. 2002. № 5-6.
75. Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность: Учебник. Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. 426 с
76. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. М.: Форум, Инфра-М, 2017. 416 с.

77. Ярочкин, В. Безопасность информационных систем / В. Ярочкин. М.: Ось-89, 2016. 320 с.
78. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с
79. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.:Горячая линия - Телеком, 2000. 452с.
80. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.
81. Зима В.М. Безопасность глобальных сетевых технологий / В.М.Зима, А.А.Молдовян, Н.А.Молдовян. СПб.; БХВ-Петербург, 2019. – 320 с
82. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.
83. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях М.: ДМК Пресс, 2012. 592 с.
84. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. М.: Триумф, 2002. 816 с.
85. Шрамко В. Н. Аппаратно-программные средства контроля доступа // PCWeek/RE. 2003. № 9.
86. Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. 2004. № 12.
87. Шрамко В. Я. Комбинированные системы идентификации и аутентификации / / PCWeek/RE. 2004. № 45.
88. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В. 2001, 352 с.
89. www.cert.az/ziyankar.html
90. www.dtx.gov.az/haqqimizda1.php
91. www.dtx.gov.az/tarix3.php 21.
92. www.ict.az
93. https://www.javatpoint.com/cyber-security-tutorial
94. https://www.cybrary.it/
95. OWASP (Açıq Web Təhlükəsizliyi Mərkəzi) - https://owasp.org/
96. SANS Institute - https://www.sans.org/
97. Infosec Institute - https://www.infosecinstitute.com/
98. HackRead - https://www.hackread.com/
99. Dark Reading - https://www.darkreading.com/
100. KrebsOnSecurity - https://krebsonsecurity.com/

101. Threatpost - https://threatpost.com/
102. SecurityWeek - https://www.securityweek.com/
103. https://www.howtonetwork.com/comptia-network-study-guide-free/
104. https://moodle.kstu.ru/mod/page/view.php?id=9364
105. https://www.coursera.org/courses?query=information%20security
106. https://en.wikipedia.org/wiki/Password_strength#Guidelines_for_strong_passwords
107. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
108. https://blog.kaspersky.com/10-worst-password-ideas-as-seen-in-the-adobe-hack/3198/
109. http://lifehacker.com/5937303/your-clever-password-tricks-arent-protecting-you-from-todays-hackers
110. https://www.random.org/passwords/
111. http://world.std.com/~reinhold/diceware.html
112. https://www.safetydetectives.com/password-meter/
113. http://www.pcworld.com/article/2858642/you-can-encrypt-your-hard-drive-but-the-protection-may-not-be-worth-the-hassle.html
114. https://answers.syr.edu/display/software/Encrypting+your+external+hard+drive+on+Windows+and+OSX
115. http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946
116. http://blogs.microsoft.com/cybertrust/2012/07/31/microsofts-free-security-tools-series-introduction/
117. https://blogs.microsoft.com/cybertrust/2013/01/15/microsoft-free-security-tools-microsoft-security-compliance-manager-tool-scm/
118. Port Checker - Check Open Ports Online (dnschecker.org)
119. https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play
120. Metasploit: http://www.metasploit.com/ also a cheat sheet for Metasploit
121. http://www.openvas.org/
122. http://lifehacker.com/198946/how-to-portscan-your-computer-for-security-holes
123. http://www.techradar.com/us/news/networking/how-to-secure-your-tcp-ip-ports-633089

124. http://www.techrepublic.com/article/lock-it-down-develop-a-strategy-for-securing-ports-on-your-servers/
125. https://www.grc.com/default.htm
126. https://www.avg.com/en/signal/prevent-router-hacking
127. http://security.stackexchange.com/questions/77112/danger-of-default-router-password
128. http://www.acunetix.com/blog/web-security-zone/the-email-that-hacks-you/
129. http://www.howtogeek.com/173921/secure-your-wireless-router-8-things-you-can-do-right-now/
130. https://portscaner.ru/protocols-ports-tcp-udp
131. https://www.geeksforgeeks.org/network-and-communication/?ref=lbp

MÜNDƏRİCAT

MÜƏLLİF HAQQINDA

Aidə Mübariz qızı Mustafayeva 1981-ci ildə Göyçə mahalının Qoşabulaq kəndində anadan olmuşdur. O, Mingəçevir Politexnik İnstitutunun "İnformasiya işlənməsinin və idarəetmənin avtomatlaşdırılmış sistemləri" ixtisası üzrə bakalavr təhsil pilləsini 2003-cü ildə, magistr təhsil pilləsini isə 2005-ci ildə fərqlənmə diplomu ilə bitirmişdir. Həmin ildə Mingəçevir Politexnik İnstitutunun "Kompüter Tədris Mərkəzinə" böyük laborant vəzifəsinə təyin edilmiş və 2006-cı ildə müsabiqə yolu ilə "Avtomatlaşdırma və informasiya texnikası" kafedrasına müəllim vəzifəsinə seçilmişdir.

2017-ci ildə AMEA-ının İdarəetmə Sistemləri İnstitutunun 333801 – "Sistemli analiz, idarəetmə və informasiyanın işlənməsi" ixtisası üzrə "Qeyri-səlis xaotik dinamik obyektlərdə idarəetmənin sintezi və təhlili" mövzusu üzrə dissertasiya işini müdafiə edərək, AAK-nın 08 iyun 2018-ci il tarixli 20№li protokol qərarı ilə texnika üzrə fəlsəfə doktoru elmi dərəcəsinə layiq görülmüşdür.2020-ci ildən eyni ixtisas üzrə elmlər doktorluğu dərəcəsini qazanmaq üçün "Süni intellekt nəzəriyyəsinin tətbiqilə çoxölçülü obyektlərdə informasiya emalının və idarəetmə üsul və vasitələrinin işlənməsi mövzusu" üzrə tədqiqat işi götürüb. Hazırda Mingəçevir Dövlət Universitetinin "İnformasiya texnologiyaları" kafedrasının müdiri vəzifəsində çalışır. Müdafiədən sonra A.Mustafayevanın 60 elmi işi var və xaricdə 33 məqalə (SCOPUS, Google Schoolar, e-library) 1 dərs vəsaitinin, 3 metodik göstəriş nəşr olunmuşdur, həmçinin 70 tədris proqramının müəllifidir. 2018-ci ildən Mingəçevir Dövlət Universitetinin İnformasiya texnologiyaları kafedrasının müdiri vəzifəsində çalışır. Müxtəlif təlimlərdə, layihələrdə kurslarda iştirak edərək, 2 Beynəlxalq və 4 yerli sertifkat qazanmışdır. Technest təqaüd proqramının "Front-End proqramlaşdırma" kursu üzrə qalibi olmuşdur. Hazırda Kibertəhlükəsizliyin əsasları, IoT texnologiyalarının əsasları, Süni intellekt və robototexnika üzrə müxtəlif kurslarda, təlimlərdə iştirak edir. Ailəlidir. İki övladı var.