Azərbaycan Respublikasının Dövlət Himni

Musiqisi Üzeyir Hacıbəylinin,
sözləri Əhməd Cavadındır.

Azərbaycan! Azərbaycan!
Ey qəhrəman övladın şanlı Vətəni!
Səndən ötrü can verməyə cümlə hazırız!
Səndən ötrü qan tökməyə cümlə qadiriz!
Üçrəngli bayrağınla məsud yaşa!
Minlərlə can qurban oldu!
Sinən hərbə meydan oldu!
Hüququndan keçən əsgər,
Hərə bir qəhrəman oldu!

Sən olasan gülüstan,
Sənə hər an can qurban!
Sənə min bir məhəbbət
Sinəmdə tutmuş məkan!

Namusunu hifz etməyə,
Bayrağını yüksəltməyə
Cümlə gənclər müştaqdır!
Şanlı Vətən! Şanlı Vətən!
Azərbaycan! Azərbaycan!

HEYDƏR ƏLİYEV
AZƏRBAYCAN XALQININ ÜMUMMİLLİ LİDERİ

Salayev Oktay Ağacan
Rəhimov Nurlan Kərim
Mirzəyeva Günel Mahir

İnformasiya sistemlərində təhlükəsizliyin təmini

Orta ixtisas təhsili müəssisələrinin tələbələri üçün dərslik

Azərbaycan Respublikası Elm və Təhsil Nazirinin 3-29/3-2-49F/2024 saylı 09.02.2024-cü il tarixli əmri ilə dərslik kimi təsdiq edilmişdir.

BAKI – 2024

Rəy verənlər: **Qasımov Vaqif Əlicavad oğlu**
Azərbaycan Texniki Universitetinin "Kompüter texnologiyaları" kafedrasının müdiri, t.e.d., professor.

Məzahir İsayev Məhəmməd oğlu
Azərbaycan Respublikası Elm və Təhsil Nazirliyi İdarəetmə Sistemləri İnstitutunun İntellektual informasiya-ölçmə sistemləri laboratoriyasının müdiri, t.e.d. professor

Nəbiyev Əmiraslan Məhəmməd oğlu
Azərbaycan Kooperasiya Universitetinin "Kompüter mühəndisliyi və informasiya texnologiyaları" kafedrasının dosenti, f.ü.f.d

Şıxalıyeva Ülviyyə Akif qızı
Sabirabad Dövlət Sosial-İqtisadi Kollecin müəllimi

Redaktor: **Salayeva Nigar Nazim qızı**
Azərbaycan Texniki Universiteti nəzdində Bakı Dövlət Rabitə və Nəqliyyat Kollecinin müəllimi

O.Salayev, N.Rəhimov, G.Mirzəyev, "İnformasiya sistemlərində təhlükəsizliyin təmini", Orta ixtisas təhsili müəssisələrinin tələbələri üçün dərslik. Birinci nəşr. Bakı–2024, «CLASS PRİNT MMC», 156 səhifə.

Müdəricat

GİRİŞ HİSSƏ

Dərslikdə informsiya təhlükəsizliyinin əsas anlayışları, kompüter sistemlərində və şəbəkələrində informasiya hədələri haqqında məlumat, onların təhlil edilməsi tutarlı səviyyədə verilir. Təhlükəsizlik siyasətinin baza anlayışları müəyyənləşdirilir. Kriptoqrafik üsullarla yanaşı kompüter informasiyasının müdafiə alqoritminə baxılır.

Korporativ şəbəkələrdə informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma əsaslandırılır. Şəbəkələrarası verilənlərin mübadiləsinin müdafiə edilməsinin baza texnologiyası izah olunur. Antivirus müdafiə və onun üsullarına baxılır. Standartlardan istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi üçün istifadə olunan təşkilatı-qanunlar ətraflı izah olunur.

VPN şəbəkələrinə və onlarda informasiya təhlükəsizliyinin təmin olunmasına aid geniş məlumatlar verilir. Bu şəbəkələrin müxtəlif şəbəkə texnologiyaları bazasında qurulması və eləcə də onların qurulmasında istifadə olunan protokolların analizi verilir.

İnformasiya mühafizəsi sistemlərinin kriptoqrafik vasitələri, mexanizmləri və modelləri işıqlandırılır. Bağlı və açıq açarlı kriptoqrafiya texnologiyalarına aid geniş və məzmunlu material dərc edilir, qorunan sistemlərə baxılır, bu sistemlərdə məlumatın əldə edilməsi, emalı, ötürülməsi və mühafizəsi, eləcə də şifrləmə, maneədavamlı kodlama və informasiyanın sıxılması məsələləri,rəqəmsal imza işıqlandırılır.

Dərslik tələbələr, subbakalavr və bu sahə üzrə məlumat almaq istəyənlər üçün nəzərdə tutlmuşdur.

§1. İnformasiya sisteminin təhlükəsizliyinin əsas anlayışları.

İnformasiya sisteminin təhlükəsizliyi sistemin məlumatın məxfiliyini və bütövlüyünü təmin etmək qabiliyyətindən ibarət olan bir xüsusiyyətdir.

İnformasiya təhlükəsizliyi dedikdə informasiyanın və informasiya mühitinin təsadüfi və ya düşünülmüş təbii və ya süni xarakterə malik təsirlərdən müdafiə vəziyyəti başa düşülür. Belə təsirlər informasiyaya və ya informasiya obyektlərinə, həmçinin informasiya istifadəçisinə və sahibinə yolverilməz ziyanlar vura bilir.

İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin olunması üçün həyata keçirilən kompleks tədbirlərdir.

Bu baxımdan dərsliyin mahiyyəti nisbətən cavan, amma dinamik inkişaf edən informasiya texnologiyaları sahələrində istifadə olunan informasiyanın müdafiə olunma modelinin və üsullarının, həmçinin bu məqsədlə istifadə edilən vasitələrinin öyrənilməsi və tədqiq edilməsidir.

İndiki zamanda informasiyanın təhlükəsizliyi informasiyanın ən çox yayılmış üç əsas xüsusiyyətinə əsaslanır:

1. Konfidensiallıq.
2. Tamlıq.
3. Əlçatanlıq.

İnformasiya sistemləri üçün təhlükələr aşağıdakı qruplarda qruplaşdırıla bilər:

- məlumatın açıqlanması təhlükəsi;
- bütövlüyün pozulması təhlükəsi ─ kompüter sistemində saxlanılan və ya bir sistemdən digərinə ötürülən

məlumatların qəsdən icazəsiz və ya qəsdən dəyişdirilməsi (silinməsi);

- xidmətdən imtina təhlükəsi ─ bəzi kompüter sistemi resursuna girişin bloklanması.

Baş vermə xüsusiyyətinə görə təhlükələr təbii və süni olaraq bölünə bilər.

Təbii təhlükələr obyektiv fiziki proseslərin və ya təbii hadisələrin İS-ə təsiri ilə bağlı təhlükələrdir. Texnogen təhlükələr insan fəaliyyəti ilə əlaqəli informasiya sisteminə təhlükədir.

İS istifadəçisi informasiya sisteminin təhlükəsizliyinə təhlükə yaradan, bilmədən aşağıdakı hərəkətləri edə bilər:

- sistemin qismən və ya tam nasazlıq vəziyyətinə gətirilməsi, sistemin aparat, proqram təminatı, informasiya ehtiyatlarının məhv edilməsi (avadanlığın, yaddaş daşıyıcılarının zədələnməsi, silinməsi, mühüm məlumat və ya proqramların, o cümlədən sistemli faylların təhrif edilməsi və s.);
- avadanlıqların qeyri-qanuni işə salınması və ya cihazların və proqramların iş rejimlərinin dəyişdirilməsi;
- səriştəsiz istifadə edildikdə sistemin funksionallığının itirilməsinə və ya sistemdə geri dönməz dəyişikliklərə səbəb ola biləcək xidmət proqramlarının işə salınması;
- rəsmi vəzifələrin yerinə yetirilməsi üçün zəruri olmayan uçota alınmayan proqramların, sonradan əsassız olaraq resursların xərclənməsi (prosessorun yüklənməsi, operativ yaddaşın və xarici daşıyıcıların yaddaşının ələ keçirilməsi) ilə qanunsuz tətbiq edilməsi və istifadəsi;
- kompüterin viruslarla yoluxması;

- məxfi məlumatların açıqlanması;
- girişə nəzarət atributlarının (parollar, şifrələmə açarları, identifikasiya kartları, keçidlər və s.) açıqlanması, ötürülməsi və ya itirilməsi;
- təşkilati məhdudiyyətlərə məhəl qoymamaq;
- informasiya təhlükəsizliyi vasitələrinin səriştəsiz istifadəsi, konfiqurasiyası və ya qeyri-qanuni sıradan çıxarılması;
- məlumatların abunəçinin (cihazın) səhv ünvanına yönləndirilməsi;
- yanlış məlumatların daxil edilməsi;
- rabitə kanallarının zədələnməsi.

İS istifadəçisi informasiya sisteminin təhlükəsizliyinə təhlükə yaradan aşağıdakı qəsdən hərəkətləri edə bilər:

- sistemin fiziki məhvi və ya onun ən vacib komponentlərinin sıradan çıxması;
- kompüter sistemlərinin (elektrik təchizatı, soyutma və ventilyasiya, rabitə xətləri və s.) fəaliyyətini təmin etmək üçün altsistemləri sıradan çıxarmaq və ya sıradan çıxarmaq;
- sistemin fəaliyyətinin qeyri-mütəşəkkilliyi (cihazların və ya proqramların iş rejimlərinin dəyişdirilməsi, güclü aktiv radio müdaxiləsinin yaradılması və s.);
- agentlərin kadrlara daxil edilməsi (o cümlədən mühafizə xidməti), kadrların və ya müəyyən səlahiyyətlərə malik olan fərdi istifadəçilərin işə götürülməsi;
- dinləmə cihazlarından istifadə, məsafədən foto və video çəkiliş və s.;
- cihazlardan və rabitə xətlərindən yan elektromaqnit, akustik və digər şüalanmaların tutulması, habelə aktiv

şüalanmanın informasiyanın emalı ilə bilavasitə iştirak etməyən köməkçi texniki vasitələrə (telefon xətləri, elektrik şəbəkələri, istilik və s.) yönəldilməsi;

- rabitə kanalları vasitəsilə ötürülən məlumatların tutulması və sistemə nüfuz etməyə cəhd etmək məqsədilə onların təhlili;
- yaddaş daşıyıcılarının oğurlanması;
- yaddaş daşıyıcılarının icazəsiz surətinin çıxarılması;
- istehsalat tullantılarının oğurlanması (çaplar, qeydlər, silinmiş saxlama vasitələri və s.);
- RAM və xarici yaddaş qurğularından qalıq məlumatların oxunması, əməliyyat sisteminin istifadə etdiyi RAM sahələrindən məlumatların oxunması;
- qeyri-qanuni yollarla parolların və digər girişə nəzarət detallarının əldə edilməsi (kəşfiyyat vasitəsilə, istifadəçilərin səhlənkarlığından istifadə etməklə, seçim yolu ilə, sistem interfeysinin imitasiya edilməsi və s.) sonradan qeydiyyatdan keçmiş istifadəçi kimi maskalanmaqla;
- unikal fiziki xüsusiyyətləri olan istifadəçi terminallarından icazəsiz istifadə;
- informasiyanın şifrələmə şifrələrinin pozulması;
- xüsusi aparat əlavələrinin, "bookmark" proqramlarının və "Troyan atlarının" tətbiqi.

Qeyd etmək lazımdır ki, çox vaxt məqsədə çatmaq üçün bədniyyətli bir üsuldan deyil, onların müəyyən birləşməsindən istifadə edir.

Bədniyyətin informasiya təhlükəsizliyinə müəyyən təhdidləri həyata keçirmək üçün imkanlar toplusunun rəsmiləşdirilmiş təsviri və ya təsvirinə müdaxilə modeli deyilir.

Bədniyyətin modelini hazırlayarkən aşağıdakı fərziyyələr edilir:

- cinayət törətmiş şəxsin aid ola biləcəyi şəxslər kateqoriyaları haqqında;
- cinayətkarın hərəkətlərinin motivləri haqqında;
- cinayət törətmiş şəxsin ixtisası və onun texniki təchizatı haqqında;
- pozucunun mümkün hərəkətlərinin xarakteri haqqında.

İS ilə əlaqədar olaraq, pozucular daxili (sistem işçiləri arasından) və ya xarici (kənar) ola bilər. Daxili pozuculara aşağıdakı kadr kateqoriyalarından olan şəxslər daxil ola bilər:

- sistem istifadəçiləri;
- texniki avadanlıqlara xidmət göstərən personal (mühəndislər, texniki işçilər);
- proqram təminatının hazırlanması və texniki xidmət şöbələrinin əməkdaşları (tətbiq və sistem proqramçıları);
- binaya xidmət göstərən texniki heyət (təmizləyicilər, elektrikçilər, santexniklar və İS komponentlərinin yerləşdiyi binaya və binalara çıxışı olan digər işçilər);
- İD təhlükəsizlik işçiləri;
- rəsmi iyerarxiyanın müxtəlif səviyyəli menecerləri. Xarici müdaxilələr ola biləcək kənar şəxslər:
- müştərilər;
- ziyarətçilər;
- təşkilatın həyatının təmin edilməsi (enerji, su, istilik təchizatı və s.) məsələləri üzrə qarşılıqlı fəaliyyət göstərən təşkilatların nümayəndələri;
- rəqabət aparan təşkilatların nümayəndələri və ya onların

göstərişi ilə hərəkət edən şəxslər;

- girişə nəzarət rejimini təsadüfən və ya qəsdən pozan şəxslər (ƏM təhlükəsizliyini pozmaq məqsədi olmadan).

Pozuntuların üç əsas motivini ayırd etmək olar: məsuliyyətsizlik, özünü təsdiqləmə və eqoist maraq.

Qanunu pozanları aşağıdakı meyarlara görə təsnif etmək olar.

1. ƏM haqqında bilik səviyyəsinə görə.

2. İmkanların səviyyəsinə görə qanun pozucuları fərqləndirilir:

- məlumat əldə etmək üçün sırf gizli üsullardan istifadə etməklə;
- passiv vasitələrdən istifadə etməklə (sistemin komponentlərini dəyişdirmədən texniki müdaxilə vasitələri);
- onu aradan qaldırmaq üçün yalnız standart vasitələrdən və mühafizə sistemlərinin çatışmazlıqlarından, habelə mühafizə postları vasitəsilə gizli şəkildə aparıla bilən yığcam maqnit saxlama mühitlərindən istifadə etməklə;
- aktiv təsir üsullarından və vasitələrindən istifadə etməklə (əlavə mexaniki vasitələrin dəyişdirilməsi və qoşulması, məlumatların ötürülməsi kanallarına qoşulması, proqram təminatının "əlfəcinlərinin" həyata keçirilməsi və xüsusi instrumental və texnoloji proqramların istifadəsi).

3. Hərəkətin keçirildiyi yerdə qanun pozucuları ola bilər:

- nəzarət edilən əraziyə çıxışı olmayan təşkilatlar;
- bina və tikililərə çıxışı olmayan nəzarət edilən ərazidən fəaliyyət göstərmək;
- qapalı şəraitdə, lakin texniki informasiya sistemlərinə

çıxış olmadan işləmək;
- Son istifadəçilərin iş yerlərindən fəaliyyət göstərən İS;
- verilənlər zonasına (verilənlər bazası, arxiv və s.) çıxış imkanı;
- İS təhlükəsizliyinin idarə olunması sahəsinə çıxışın olması.

Təhlükəsizlik sistemi informasiya təhlükəsizliyini təmin etmək üçün nəzərdə tutulmuş xüsusi hüquqi və inzibati tədbirlərin, təşkilati tədbirlərin, proqram təminatı və texniki vasitələrin mühafizəsi vasitələrinin, habelə xüsusi personalın məcmusudur.

Effektiv mühafizə sistemi qurmaq üçün aşağıdakı işləri yerinə yetirmək lazımdır:
- informasiya təhlükəsizliyinə təhdidləri müəyyən etmək;
- məlumat sızmasının və məlumatlara icazəsiz girişin (NAA) mümkün kanallarını müəyyən etmək;
- potensial pozucunun modelini qurmaq;
- müvafiq mühafizə tədbirlərini, metodlarını, mexanizmlərini və vasitələrini seçmək.

İnformasiya təhlükəsizliyi sisteminin yaradılması probleminə iki vəzifə daxildir:
- informasiya təhlükəsizliyi sisteminin inkişafı;
- hazırlanmış informasiya təhlükəsizliyi sisteminin qiymətləndirilməsi.

İkinci vəzifə, informasiya təhlükəsizliyi sisteminin bir sıra tələblərə cavab verib-vermədiyini müəyyən etmək üçün sistemin texniki xüsusiyyətlərini təhlil etməklə həll edilir. Bu vəzifə hazırda ekspertlər tərəfindən informasiya təhlükəsizliyi vasitələrinin sertifikatlaşdırılması və onun həyata keçirilməsi prosesində informasiya təhlükəsizliyi sisteminin sertifikatlaşdırılması yolu ilə həll edilir.

İnformasiya təhlükəsizliyi metodlarının əsas məzmunu:

1. Maneələrin yaradılması ─ təcavüzkarın qorunan məlumatlara (avadanlıq, saxlama vasitələri və s.) gedən yolunu fiziki olaraq bloklamaq üsulları.
2. Girişə nəzarət kompüterin informasiya sisteminin bütün resurslarından (məlumat bazası elementləri, proqram təminatı və texniki vasitələrin) istifadəsini tənzimləməklə informasiyanın mühafizəsi üsuludur.
3. Kompüter resurslarına icazəsiz daxil olmaqdan mühafizə aşağıdakı məsələlərin həllini nəzərdə tutan mürəkkəb problemdir:

- istifadəçilərə, terminallara, proqramlara, fayllara və rabitə kanallarına unikal adların və kodların (identifikatorların) təyin edilməsi;
- informasiya sisteminə daxil olarkən autentifikasiya prosedurlarının yerinə yetirilməsi, yəni identifikatoru təqdim edən şəxsin və ya cihazın ona faktiki uyğunluğunun yoxlanılması;
- səlahiyyətin yoxlanılması, yəni istifadəçinin sistemə və ya tələb olunan məlumatlara daxil olmaq hüququnun yoxlanılması;
- istifadəçi identifikatoru, terminal, sorğunun vaxtı və xarakteri göstərilməklə informasiya resurslarına edilən həm təmin edilmiş, həm də rədd edilmiş bütün sorğuların xüsusi jurnalda avtomatik qeydiyyatı, yəni audit.

4. Maskalama informasiyanın kriptoqrafik şəkildə bağlanması yolu ilə qorunması üsuludur.
5. Tənzimləmə ─ mühafizə olunan məlumatların avtomatlaşdırılmış işlənməsi, saxlanması və ötürülməsi üçün şərait yaradan informasiyanın mühafizəsi metodu,

onun əsasında ona icazəsiz daxil olma ehtimalı minimuma endirilir.

6. Məcburiyyət, istifadəçilərin və sistem işçilərinin maddi, inzibati və ya cinayət məsuliyyəti təhlükəsi altında qorunan məlumatların emalı, ötürülməsi və istifadəsi qaydalarına riayət etməyə məcbur edildiyi mühafizə üsuludur.

Nəzərdən keçirilən təhlükəsizlik üsulları texniki, proqram təminatı, təşkilati və qanunvericilik kimi müxtəlif təhlükəsizlik tədbirlərinin tətbiqi ilə praktikada həyata keçirilir.

§2. İnformasiya təhlükəsizliyinin standart təyinatları. İnformasiya təhlükəsizliyinin təmini üsulları və vasitələri

İnformasiyanın qorunması — informasiyanın gizliliyinin, tamlığının və ona girişin (əlyetərliliyin) təmin edilməsidir.

İnformasiyanın qorunmasının məqsədləri aşağıdakılardan ibarətdir:

- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- dövlət sirri təşkil edən və məxfi informasiyanın məxfiliyinin qorunması;
- informasiyanın məhvinin, itməsinin, təhrif edilməsinin, saxtalaşdırılmasının, surətinin çıxarılmasının,

qarşısının alınması;

Qanunvericilik səviyyəsində hüquqi aktlar və standartlar xüsusi diqqətə layiqdir. Standrtların arasında «Narıncı kitab», X.800 tövsiyələri, ISO 15408 («Ümumi meyarlar»), ISO 17799 standartları daha geniş yayılıb. İnzibati tədbirlərin əsas məqsədi təşkilatda informasiya təhlükəsizliyi sahəsində tədbirlər proqramını formalaşdırmaq və onun yerinə yetirilməsini zəruri resurslar ayırmaqla və işlərin vəziyyətinə nəzarət etməklə yerinə yetirilməsini təmin etməkdir.

Tədbirlər proqramının əsasını təşkilatın öz informasiya aktivlərinin mühafizəsinə yanaşmasını əks etdirən informasiya təhlükəsizliyi siyasəti təşkil edir. Narıncı kitab İnformasiya təhlükəsizliyi sahəsində tarixən ilk standart ABŞ Müdafiə Nazirliyinin "Etibarlı kompüter sistemlərinin qiymətləndirilməsi meyarları" olmuşdur. Cildinin rənginə görə çox vaxt "Narıncı kitab" adlanan bu standart ilk dəfə 1983-cü ilin avqustunda nəşr edilmişdi. "Narıncı kitabda" etibarlı sistemi "giriş hüququnu pozmadan müxtəlif məxfilik dərəcəsinə malik informasiyanın istifadəçilər qrupu tərəfindən eyni zamanda emalını təmin etmək üçün yetərli aparat və proqram təminatı istifadə edən sistem" kimi müəyyən edir.

"Narıncı kitabda" dörd etibar səviyyəsi – D, C, B və A müəyyən edilir.

D səviyyəsi qeyri-qənaətbəxş qəbul edilmiş sistemlər üçün nəzərdə tutulub. C səviyyəsindən A səviyyəsinə keçdikcə sistemlərə daha ciddi tələblər irəli sürülür. C və B səviyyələri etibar dərəcəsinin tədricən artması ilə siniflərə bölünür (C1, C2, B1, B2, B3).

"Narıncı kitabda" daxil edilmiş təsnifatı qısaca belə ifadə

etmək olar:

- C səviyyəsi – girişin ixtiyari idarə edilməsi;
- B səviyyəsi – girişin mandatlı idarə edilməsi;
- A səviyyəsi – təhlükəsizliyin verifikasiya edilə bilməsi.

"Narıncı kitabın" hamı tərəfindən qəbul edilən anlayışlar bazisi meydana çıxartdı ki, bunlarsız informasiya təhlükəsizliyi məsələlərinin hətta müzakirəsi belə çətin olardı.

ISO/IEC 15408 standartı

Qiymətləndirmə standartlarının içərisində ən tamı və müasiri İSO/İEC 15408 "İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları" standartıdır (1 dekabr 1999cu ildə nəşr olunmuşdur). Bu beynəlxalq standart bir neçə ölkə mütəxəssisinin demək olar ki, onillik işinin nəticəsidir, o özündə həmin dövrə mövcud olan beynəlxalq və milli standartların təcrübəsini cəmləşdirmişdir.

Tarixi səbəblərdən bu standartı çox zaman "Ümumi meyarlar" adlandırırlar. Biz də bu qisaltmadan istifadə edəcəyik. "Narıncı kitab"dakı kimi Ümumi meyarlarda da təhlükəsizlik tələblərinin iki əsas növü var:

- funksional tələblər və zəmanət tələbləri – mühafizənin aktiv aspektinə uyğundur, təhlükəsizlik funksiyalarına və onları realizə edən mexanizmilərə uyğun olaraq irəli sürülür;
- mühafizənin passiv aspektinə uyğundur, yaradılma və istismar texnologiyasına və prosesinə uyğun olaraq irəli sürülür.

Funksional tələblər

Funksional tələblər aşağıdakı sinifləri müəyyən edilir.

- Təhlükəsizliyin auditi;

- Kommunikasiya;
- Kriptoqrafik dəstək;
- İdentifikasiya və autentifikasiya;
- Konfidensiallıq.

Funksional tələblərin ingilis dilində ixtisarlarla işarə edilən aşağıdakı sinifləri müəyyən edilir.

- Təhlükəsizliyin auditi (FAU). Təhlükəsizlik sisteminin auditi – təhlükəsizlik sisteminə aid informasiyanın tanınması, qeydə alınması, saxlanması və analizidir.
- Kommunikasiya (FCO). Bu sinfin tələblərinin yerinə yetirilməsi zəmanət verir ki, informasiyanı göndərən ötürülən informasiyadan, qəbuledən isə onu aldığından imtina edə bilməz.
- Kriptoqrafik dəstək (FCS). Sinifdə kriptoqrafik açarların və əməliyyatların idarə edilməsi üzrə tələblər var.
- İstifadəçinin verilənlərinin mühafizəsi (FDP). Sinif informasiyanı daxiletmə, xaricetmə və saxlama zamanı istifadəçi verilənlərinin mühafizəsinə aid təhlükəsizlik tələblərini müəyyən edir.
- İdentifikasiya və autentifikasiya (FIA). Bu sinfin tələbləri sistemdə istifadəçilərin müəyyən edilməsi və verifikasiyası ilə, onların sistemdə səlahiyyətləri ilə, həmçinin təhlükəsizlik atributlarının hər bir istifadəçiyə düzgün verilməsi ilə işləyir.
- Təhlükəsizliyin idarə edilməsi (FMT). Sinfə təhlükəsizlik funksiyaları verilənlərinin və atributlarının, həmçinin təhlükəsizlik rollarının idarə edilməsi üzrə tələblər daxildir.
- Konfidensiallıq (FPR). Bu sinfin tələblərinin realizə

edilməsi istifadəçini onun səlahiyyətlərinin digər istifadəçilər tərəfindən açılmasından və sui-istifadə edilməsindən mühafizə edəcək.

- Təhlükəsizlik funksiyalarının mühafizəsi (FPT). Sinfə sistemin təhlükəsizlik mexanizmlərinin tamlığına və idarə edilməsinə aid funksional tələblər daxildir (realizə edilən təhlükəsizlik siyasətindən asılı olmayaraq).
- Resursların istifadəsi (FRU). Bu sinfin tələbləri lazımi resursların əlyetənliyini (emal /və ya saxlama imkanı kimi), həmçinin sistemin imtinaları ilə funksional imkanların meydana çıxan bloklanması halında mühafizəni təmin edir.
- Qiymətləndirmə obyektinə giriş (FTA). Sinif istifadəçinin təyin edilmiş iş seansına funksional nəzarət tələblərini identifikasiya və autentifikasiya üzrə tələblərdən asılı olmadan müəyyən edir.
- Etibarlı marşrut/kanal (FTP). Sinif aşağıdakı tələbləri təmin edir:

  1. Istifadəçi ilə sistemin təhlükəsizlik funksiyaları arasında etibarlı kommunikasiya marşrutu;

  2. sistemin təhlükəsizlik funksiyaları arasında etibarlı rabitə kanalı.

Zəmanət tələbləri

Standart aşağıdakı zəmanət siniflərini daxil edir:

- Konfiqurasiyanın idarə edilməsi;
- Çatdırılma və istismar;
- Yaratma və Testlər;
- Rəhbər sənədlər;
- Boşluqların qiymətləndirilməsi.

Standart ingilis dilində ixtisarlarla adlandırılmış

aşağıdakı zəmanət siniflərini daxil edir:

- Konfiqurasiyanın idarə edilməsi (ACM). Ümumi Meyarlar qiymətləndirilən obyektin tamlığının saxlanmasını onun dəqiqləşdirilməsi və modifikasiyası zamanı idarəetmə və intizam tələb etməklə təmin edir.
- Çatdırılma və istismar (ADO). ADO zəmanət sinfi qiymətləndirilən obyektin etibarlı çatdırılması, qurulması və istismar istifadəsinə aid tədbirlərə, prosedurlara və standartlara tələbləri müəyyən edir.
- Yaratma (ADV). Bu zəmanət sinfi qiymətləndirilən obyektin ümumi spesifikasiyasından təhlükəsizlik funksiyalarının faktiki realizəyə yuxarıdan aşağıya addım-addım dəqiqləşdirilməsi üzrə tələbləri müəyyən edir.
- Rəhbər sənədlər (AGD). Bu zəmanət sinfi istehsalçının təqdim etdiyi istismar sənədlərinin anlaşıqlıq və tamlıq tələblərini müəyyən edir.
- Həyat dövrünün dəstəklənməsi (ALC). Bu sinif qiymətləndirilən obyektin yaradılmasının bütün addımları üçün həyat dövrü modelini, o cümlədən qüsurların aradan qaldırılması prosedurlarını və siyasətini dəqiq müəyyən edir.
- Testlər (ATE). Bu zəmanət sinfi təhlükəsizlik funksiyalarının funksional təhlükəsizlik tələblərini ödədiyini nümayiş etdirən sınaqlara tələbləri müəyyən edir.
- Boşluqların qiymətləndirilməsi (AVA). Bu zəmanət sinfi istismar zamanı qalan zəif yerlərin identifikasiyasına yönəlmiş tələbləri müəyyən edir.
-

İnformasiya təhlükəsizliyinin təmini üsulları

İnformasiya təhlükəsizliyinin sistemlərinin hazırlaması sahəsində fəaliyyət göstərən Kasperiski laboratoriyasının ekspertlərinin fikrincə informasiya təhlükəsizliyi məsələləri sistemli həll olunmalıdır. Bu o deməkdir ki, müxtəlif mühafizə vasitələri (aparat, proqram, fiziki, təşkilati və s.) eyni vaxtda mərkəzi idarə olunmaqla tətbiq olunmalıdır. Bu zaman sistemin mühafizə vasitələri bir-birinin mövcüd olmasını bilməli, qarşılıqlı təsirli olmalı və həm xarici, həm də daxili həmlələrdən mühafizəsini təmin etməlidir. Bu gün informasiya təhlükəsizliyini təmin edən çoxlu sayda üsullar mövcuddur.

Bunlara misal olaraq aşağıdakı üsulları göstərmək olar:

- istifadəçilərin identifikasiyası və autentifikasiyası (buna 3A kompleksi deyilir) vasitələri;
- kompyuterdə saxlanılan və şəbəkə ilə ötürülən informasiyanın şifləmə vasitələri;
- şəbəkəarası ekranlar;
- virtual şəxsi şəbəkələr;
- kontent filtirləmə vasitələri;
- disklərin məzmunlarının tamlığını yoxlayan alətlər; -
- antivirus mühafizə vasitələri;
- şəbəkələrin zəif yerlərinin aşkarlanma sistemləri və şəbəkə hücumları analizatorları.

Qeyd edilən vasitələrin hər birisi həm sərbəst, həm də başqalarına inteqrasiya olunması formasında istifadə oluna bilərlər. Bu isə istifadə olunan platformadan asılı olmayaraq istənilən mürəkkəb və konfiqurasiyalı şəbəkələr üçün informasiya mühafizəsi sistemini yaratmağa imkan verir.

3A kompleksi‖ autentifikasiyadan (və identifikasiya),

avtorlaşma və administratorlaşmadan ibarətdir.

İdentifikasiya və avtorlaşma-bunlar informasiya təhlükəsizliyinin əsas elementləridirlər. İnformasiya aktivlərinə dostup zamanı identifikasiya funksiyası belə suallara cavab verir: —Siz kimsiniz? və —siz haradasınız, siz şəbəkənin avtorlaşmış istifadəçisinizmi? Avtorlaşma funksiyası konkret istifadəçini hansı resurslara dostupunun olmasına cavab verir. Administratorlaşma funksiyasının vəzifəsi verilmiş şəbəkə daxilində istifadəçinin müəyyən identifikasiya xüsusiyyətlərinə görə bölmək və onun üçün icazəli olan həcmi müəyyən etməkdir.

Şifrələmə sistemi sərt diskdə və ya başqa bir daşıyıcıda saxlanılan verilənlərə sanksiya olunmamış (icazəsiz) dostuplar zamanı itgiləri, eyni zamanda, elektron poçt və ya şəbəkə protokolları vasitəsilə informasiyanı göndərən zaman onun ələ keçirilməsini minimuma endirməyə imkan verir. Bu mühafizə vasitələrinin vəzifəsi konfidensiallığın təminidir. Şifrələmə sisteminə qoyulan əsas tələblər-kriptodayanıqlılığın yüksək səviyyəsi və dövlətin ərazisində istifadəsinin leqallığıdır. Şəbəkəarası ekran iki və ya daha çox şəbəkə arasında mühafizə hasarı təşkil edən sistem və sistemlər kombinasiyasıdır. Verilənlər paketinin sanksiyasız şəbəkəyə düşməsinin və ya ondan çıxmasının qarşısını alır. Şəbəkəarası ekranların əsas iş prinsipi-hər bir verilənlər paketinin daxil olan və xaric olan İP-ünvanların icazə verilmiş ünvanlar bazasına uyğunluğunu aşkarlamaqdan ibarətdir.

Beləliklə, şəbəkəarası ekranlar informasiya şəbəkələrinin seqmentləşməsinə və verilənlərin dövr etməsinə nəzarət imkanını kifayət qədər genişləndirir. Kriptoqrafiya və şəbəkəarası ekranlar haqqında danışanda

mühafizə olunan virtual şəxsi şəbəkələrdən (VPN) də danışmaq lazımdır. VPN-dən istifadə verilənləri açıq kommunikasiya kanalları vasitəsilə ötürən zaman onların konfidensiallıq və tamlıq problemlərini həll etməyə imkan verir:

- kompaniyanın müxtəlif ofisləri arasında informasiya axınlarının mühafizəsi (informasiyanın şifrələnməsi yalnız xarici şəbəkəyə çıxış zamanı aparılır);
- uzaq şəbəkə istifadəçilərinin kompaniyanın resurslarına dostupu, adətən, internet üzərindən aparılır;
- korporativ şəbəkə daxilində ayrı-ayrı əlavələr arasında informasiya axınının mühafizəsi vasitəsi - daxil və xaric olan elektron poçtların məzmununun filtrləşdirilməsidir. Kontent filtrasiya vasitələri istifadə olunan bütün formatları, o cümlədən sıxılmış və qrafiki yoxlamağa imkan verir. Bu zaman şəbəkənin buraxma qabiliyyəti praktiki olaraq dəyişmir.

İşçi stansiyada və ya serverdə bütün dəyişikliklər sərt diskin məzmununun tamlığının yoxlanması texnologiyasına əsasən şəbəkə administratoru və ya başqa avtorizasiya olunmuş istifadəçilər tərəfindən izlənə bilər. Bu fayllarla olan istənilən hərəkətləri və virusların aktivliyini identifikasiya edir, sanksiya olunmamış dostupları və ya avtorlaşmış istifadəçilərin verilənləri oğurlamasını aşkarlamağa imkan verir. Nəzarət fayllar cəminin analizi (CRC cəmi) əsasında aparılır.

İnformasiya təhlükəsizliyi vasitələri

Personal (işçi personal)-bu vasitədir, auditmexanizmdir, qeydiyyat (hesabat) isə məqsəddir. Başqa bir halda autentifikasiyanı təmin edən parollar şifrələnmiş formada

saxlanılır, autentifikasiya öndə gəlir (sələfdir), misal üçün, modifikasiyaya icazə üçün. Kriptoqrafiya parolların mühafizə vasitəsidir, parollar autentifikasiya mexanizmi üçün istifadə edilir, autentifikasiya tamlığın təminindən öndə olur.

Beləliklə, informasiya təhlükəsizliyinin əsas vasitələri (alətləri) aşağıdakılardır:

- personal - bütün aspektlərdə, başqa sözlə, işləmək, tətbiq etmək, dəstəkləmək, nəzarət etmək və yerinə yetirmək informasiya təhlükəsizliyini həyata keçirən insanlardır;
- normativ təminat - informasiya təhlükəsizliyinin işlənməsi üçün hüquqi fəzanı yaradan sənədlər;
- təhlükəsizlik modelləri - verilmiş konkret informasiya sisteminə və ya mühitinə qoyulmuş informasiya təhlükəsizliyinin təmini sxemləri;
- kriptoqrafiya - informasiyanın elə çevrilmə üsul və vasitələridir ki, onunla sanksiya olunmamış əməliyyatları (oxuma və ya modifikasiya etmə) çətinləşdirir və ya imkan vermir. Təbii ki, bu üsul və vasitələr bu sanksiyaları reallaşdıran xüsusi informasiya obyektləri-açarların yaradılması, saxlanması və paylanması üsul və vasitələri ilə birgə işləyirlər;
- antivirus təminatı - təhlükəli kodların (viruslar, troyan proqramları və s.) aşkarlayıb məhv etmək üçün vasitələr;
- şəbəkəarası ekranlar - bir informasiya şəbəkəsindən başqasına dostupa nəzarət qurğusu;
- təhlükəsizlik skanerləri - konkret informasiya sistemi üçün təhlükəsizlik modelinin işləmə keyfiyyətini yoxlayan qurğu;
- həmlələri aşkarlayan sistemlər - informasiya mühitində aktivlik monitorinqi qurğusu (bəzi hallarda göstərilən

aktiv fəaliyyətdə sərbəst iştirak etmək imkanı ilə);

- ehtiyat kopiyalaşdırma - mümkün olan itirmə və ya zədələnmə zamanı istifadə etmək üçün informasiya resurslarının izafi nüsxələrinin (kopiyalarının) saxlanması;
- rezervləşdirmə - əsas qurğuların işdən çıxdığı zaman informasiya mühitinin işlək olması üçün lazım olan alternetiv qurğuların yaradılması;
- qəza planı - informasiya təhlükəsizliyi plan və vasitələrində nəzərdə tutulmuş qaydalardan kənar hallarda həyata keçirmək üçün nəzərdə tutulmuş tədbirlər yığımı;
- istifadəçilərin öyrədilməsi - informasiya təhlükəsizliyi tələblərinə uyğun şəraitdə işləmək üçün informasiya mühitinin aktiv iştirakçılarının hazırlanması.

İnformasiyanın texniki vasitələrlə mühafizəsi İnformasiyanın mühafizəsinin texniki vasitələr qrupuna apartat və proqram vasitələri aid edilir. Texniki tədbirlərin kompleksinə, kompüter sistemlərinin və şəbəkəsinin obyektlərinin fiziki əlçatanlığını təmin etmək üçün tədbirlər, məsələn, kamera avadanlıqları və siqnalizasiya kimi praktiki üsullar da daxildir.

§3. Kompüter sistem və şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsi

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi səviyyəsinin təhlili və qiymətləndirilməsi bir sıra amillərdən asılıdır. Belə ki, bunun üçün risklərin qiymətləndirilməsi, idarə edilməsi, potensial təhlükələrin və mümkün zəif yerlərin aşkar olunması, informasiya təhlükəsizliyinin təhlili kriterilərinin, üsullarının, vasitələrinin və xüsusi- ləşdirilmiş alətlərin olması, müxtəlif proqram-aparat platformaların peşəkar səviyyədə tətbiqi tələb olunur.

KSŞ-nin təhlükəsizliyinin qiymətləndirilməsinə mexanizmləri məsələnin formallaşdırılması ilə bağlı qarşıya çıxan çətinliklərə görə, praktiki olaraq, geniş yayılmamışdır.

KSŞ-nin qorunması səviyyəsi bir neçə amilin qiymətləndirilməsi yolu ilə müəyyən olunur:

- təhdidlərin həyata keçirilməsinin hər bir yolunun müvafiq qoruma mexanizmi ilə bağlanması – praktikada informasiya resurslarına münasibətdə dəqiq qiymətləndirilməsi mümkün olmayan çoxlu sayda təhdidlərini həyata keçirilməsi yolları mövcuddur.
- mövcud qoruma mexanizmlərinin möhkəmliyi – həmin mexanizmlərin adlanmasının və ya onlardan yan keçilməsinin qeyri-mümkünlüyü dərəcəsi ilə xarakterizə olunur.
- təhlükəsizliyə qarşı təhdidlər müvəffəqiyyətlə reallaşdırıldıqda informasiya resursunun sahibinə vurulan ziyanın miqdarı.

Təhlükənin mövcudluğu, ziyanın baş verməsi və qoruma

mexanizminin müqavimət göstərməsi dərəcələrini müəyyən etmək çətin olduğuna görə, adətən, bu xarakteristikaların dəqiq qiymətlərinin alınması çox çətin olur. Məsələn sosial, siyasi, hərbi, informasiya və digər sahələrdə icazəsiz giriş nəticəsində dəyən ziyanın miqdarını qiymətləndirmək ümumiyyətlə mümkün deyil. Təhlükələrin baş verməsi ehtimalı statistik analizə əsaslana bilməz. Qoruma mexanizmlərinin müqavimət göstərməsi dərəcəsinin qiymətləndirilməsi isə həmişə subyektiv xarakter daşıyır.

Bu məqsədlə çox vaxt qeyri-formal təsnifatlandırma mexanizmlərindən istifadə olunur. Həmin yanaşmalar dəyərlərin qiymətləndirilməsi əvəzinə pozucuların (məqsədlərinə, ixtisas dərəcəsinə və resurslara giriş hüquqlarına görə), informasiyanın (mühümlük və məxfilik dərəcələrinə görə), qoruma vasitələrinin (realizə olunan imkanlarına, fəaliyyətlinə və zəmanətliliyinə görə) və s. kateqoriyalara bölünməsi prinsipləri əsasında qurulur.

Qeyd olunmalıdır ki, belə yanaşma qorunma dərəcəsinin müəyyən edilməsi üçün göstəricilərin dəqiq qiymətlərini vermir, lakin qorunma səviyyəsinə görə KSŞ-ni təsnifatlandırmağa və onların müqayisəli təhlilini həyata keçirməyə imkan verir.

Burada informasiya təhlükəsizliyi sisteminin (İTS) modelinə əsaslanan, təhlükələrin baş verməsi risklərini müəyyən etməyə və onun əsasında qorunma səviyyəsinin qiymətləndirməyə imkan verən üsula baxılır.

İTS-in formal təsviri üçün təhlükələrin qarşısının alınmasına əsaslanan modeldə informasiya təhlükəsizliyi sistemi “O,T,M “ üçlüyü şəklində müəyyən olunur. Burada O – sistemin qorunan obyektləri (resursları) çoxluğu, T –

təhlükələr çoxluğu, M – informasiya təhlükəsizliyinin təmin edilməsi üsulları çoxluğudur.

İnformasiya təhlükəsizliyinin təmin edilməsi səviyyəsini təhlil etmək üçün yuxarıda qeyd olunan modelin genişlənmiş variantı təklif olunur. Burada modelə daha iki element daxil edilir. V – zəif yerlər çoxluğu, B – qoruma sədləri çoxluğudur.

Qorunmanın qiymətləndirilməsi kriterilərini və qoruma mexanizmlərinə qoyulan tələblərin müəyyən edilməsi üçün beynəlxalq səviyyədə qəbul olunmuş bir sıra normativ sənədlərdən istifadə edilir. Bu sənədlər arasında daha əhəmiyyətli yer tutan normativ sənədlər qismində "İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumu kriteriləri" (ISO 15408 – The Common Criteria for Information Technology Security Evaluation), "İnformasiya təhlükəsizliyinin idarə edilməsinin praktiki qaydaları" (ISO 17799 – Code of practice for Information security management) göstərmək olar.

İnformasiya təhlükəsizliyinin təmin edilməsi dərəcəsi

Qeyd olunduğu kimi, bu gün telekommunikasiya sistemlərinin və kompüter şəbəkələrinin təhlükəsizliyinin təmin edilməsi dərəcəsinin təhlili üçün hər hansı standartlaşdırılmış metodika mövcud deyil. Ona görə də ayrı-ayrı konkret hallarda istifadə olunan yanaşmalar əhəmiyyətli dərəcədə fərqlənə bilər. Lakin, buna baxmayaraq, aparılmış araşdırmalar göstərir ki, korporativ şəbəkələrin təhlükəsizliyinin təmin edilməsinin təhlili üçün təxmini metodika vermək mümkündür. Bu metodikaya aşağıdakı üsulların istifadəsi daxildir:

- telekommunikasiya sistemi və ya kompüter şəbəkəsi

üzrə ilkin məlumatların öyrənilməsi;

- telekommunikasiya sisteminin və ya kompüter şəbəkəsinin resurslarına münasibətdə təhlükəsizliyə təhlükələrin baş verməsi ilə bağlı risklərin qiymətləndirilməsi;
- təşkilatın informasiya təhlükəsizliyi siyasətinin, təhlükəsizliyin təşkilati üsullarının təhlili, onların normativ sənədlərin tələblərinə uyğunluğunun, eləcə də mövcud risklərə adekvatlığının qiymətləndirilməsi;
- şəbəkə infrastrukturunun marşrutlayıcıların, proksi-serverlərin, poçt və DNS-serverlərin konfiqurasiya fayllarının, digər mühüm elementlərin əl ilə təhlil edilməsi;
- lokal şəbəkənin xarici şəbəkə ünvanlarının skanlanması;
- lokal şəbəkənin resurslarının daxildən skanlanması;
- xüsusi proqram agentlərinin köməyi ilə serverlərin və işçi stansiyaların konfiqurasiyasının təhlili.

Sadalanan texniki üsullar təhlükəsizlik sisteminin həm fəal, həm də passiv testləşdirilməsini nəzərdə tutur. Fəal testləşdirmə potensial ziyankarın hərəkətlərinin emulyasiyasından ibarətdir.

Passiv testləşdirmə isə yoxlama siyahılarını istifadə etməklə şablonlar üzrə əməliyyat sisteminin və əlavələrin konfiqurasiyasının təhlilini nəzərdə tutur. Testləşdirmə əl ilə və ya xüsusi proqram vasitələrini istifadə etməklə yerinə yetirilə bilər.

Rəhbər sənədlərə uyğun olaraq, ümumi halda informasiyalaşdırma obyektinin qorunmasının tədqiqi və təhlili üçün aşağıdakı ilkin məlumatlar tələb olunur:

- informasiyalaşdırma obyektinin tam və dəqiq adı,

onun təyinatı;
- emal olunan informasiyanın xarakteri (elmi-texniki, iqtisadi, istehsal, maliyyə, hərbi, siyasi) və onun məxfilik dərəcəsi;
- informasiyalaşdırma obyektinin təşkilati strukturu və ümumi funksional sxemi;
- informasiyalaşdırma obyektinə daxil olan və informasiyanın emal olunduğu texniki vasitələr kompleksinin tərkibi;
- informasiyalaşdırma obyektinin xüsusiyyətləri və yerləşmə sxemi (nəzarət olunan zonanın sərhədini göstərməklə);
- informasiyalaşdırma obyektində istifadə olunan və informasiyanın emalı üçün nəzərdə tutulan proqram təminatının strukturu;
- informasiya mübadiləsi protokolları;
- digər informasiyalaşdırma obyektləri ilə qarşılıqlı əlaqələrin mövcudluğu və xarakteri;
- informasiyalaşdırma obyektində informasiya təhlükəsizliyi sisteminin tərkibi və strukturu, informasiya təhlükəsizliyi xidmətinin mövcudluğu;
- informasiyalaşdırma obyektində qorunan texniki və proqram vasitələrinin, qoruma və nəzarət vasitələrinin siyahısı, onların istehsalçıları haqqında məlumatlar;
- informasiyalaşdırma obyektinin fiziki qorunmasının mövcudluğu və əsas xarakteristikaları;
- informasiyalaşdırma obyektinin layihə və istismar sənədlərinin mövcudluğu haqqında məlumat.

Telekommunikasiya sisteminin və kompüter şəbəkəsinin xarici perimetri üzrə qoruma və şəbəkələrarası

qarşılıqlı əlaqələrin idarə olunması vasitələrinin konfiqurasiyasının təhlili zamanı aşağıdakı aspektlərə xüsusi fikir verilməlidir:

- girişin məhdudlaşdırılması qaydalarının qurulması;
- autentifikasiyanın istifadə olunan sxemləri və parametrlərinin qurulması;
- hadisələrin qeydiyyatı sisteminin parametrlərinin qurulması;
- qorunan şəbəkənin topologiyasının gizlədilməsini təmin edən mexanizmlərdən istifadə edilməsi;
- hücumlar haqqında məlumatların xəbərdar edilməsi mexanizmlərinin qurulması;
- bütövlüyün yoxlanması vasitələrinin mövcudluğu və iş qabiliyyəti;
- istifadə olunan proqram təminatının versiyaları və quraşdırılmış yeniliklər.

Bu proses yüzlərlə müxtəlif parametrlərin sazlanmasının düzgünlüyünün yoxlanmasını nəzərdə tutur. Paylanmış telekommunikasiya sistemlərinin və kompüter şəbəkələrinin qorunmasının təhlili və nəzarət edilməsi prosesinin avtomatlaşdırılması üsullarından biri intellektual proqram agentlərindən istifadə olunmasından ibarətdir. Bu halda nəzarət olunan sistemlərin hər birinə proqram agenti quraşdırılır. Bu agentlər proqram təminatının müvafiq qurulmasını yerinə yetirir, onların düzgünlüyünü yoxlayır, faylların bütövlüyünə, yeniləşmələrin vaxtında aparılmasına nəzarət edir, eləcə də informasiya sisteminin qorunmasının nəzarət edilməsi üzrə digər məsələləri həll edir.

Agent proqramlarının idarə olunmasını şəbəkə vasitəsilə proqram-menecer tərəfindən həyata keçirir. Belə

sistemlərdə mərkəzi komponent rolunu oynayan menecer proqramları bütün agentlərə idarəedici əmrlər göndərir və agentlərdən aldığı bütün məlumatları mərkəzi bazada saxlayır. Sistemin inzibatçısı konsol vasitəsilə menecer proqramını idarə edir, təhlükəsizlik siyasətini seçir, kökləyir və yaradır, sistemin vəziyyətinə baş verən dəyişiklikləri təhlil edir, zəiflikləri (zəif yerləri) əhəmiyyətinə görə düzü və s.

Kompüter sistemlərinin və şəbəkələrinin informasiya təhlükəsizliyinin vəziyyətinin həll edilməsi vasitələri

Daimi və ya müvəqqəti fiziki qoşulmaların mövcudluğu şəbəkədə emal olunan məlumatların sızmasının artmasına təsir edən əsas amillərdən biridir. Belə ki, informasiyanın sızması qoruma vasitələrində səhvlərin olması səbəbindən, eləcə də personalın səhv və ya səhlənkar hərəkətləri nəticəsində qərəzsiz şəkildə baş verə bilər.

Qeyd etmək lazımdır ki, təhlükəli informasiya təsirlərinin aşkarlanması tədbirlərini İTS fəaliyyətə başlamazdan əvvəl həyata keçirmək lazımdır. Ona görə də sistemin qorunmasının təhlili üsulları ilə yanaşı məlumatların təftiş edilməsi üsullarının tətbiqi informasiya resurslarının kompleks şəkildə qorunmasını təmin etməyə imkan verir.

İTS onda istifadə olunan qoruma mexanizmlərinin effektivliyinin və mümkün hücumlara münasibətdə dayanıqlılığının yoxlanılması, eləcə də qoruma baxımından zəif yerlərin müəyyən olunması məqsədilə sınaqdan keçirilir. Ənənəvi olaraq, iki sınaq üsulundan istifadə olunur:

- "qara qutu" üsulu ilə sınaq;
- "ağ qutu" üsulu ilə sınaq.

"Qara qutu" üsulu ilə sınaq zamanı nəzərdə tutulur ki, onu həyata keçirən tərəfdə sınaq obyektinin konfiqurasiyası və daxili strukturu haqqında hər hansı xüsusi biliklər yoxdur. Bu zaman sınaq obyektinə qarşı bütün məlum hücumlar reallaşdırılır və təhlükəsizlik sisteminin bu hücumlara münasibətdə dayanıqlılığı yoxlanılır. İstifadə olunan "qara qutu" üsulu sistemi sındırmağa çalışan potensial ziyankarın hərəkətlərini modelləşdirir. Bu halda əsas sınaq vasitəsi qismində məlum zəif yerlər haqqında məlumat bazasına malik olan şəbəkə skanerlərindən istifadə olunur.

"Ağ qutu" üsulu sınaq obyektinin konfiqurasiyası və daxili strukturu haqqında biliklərin bazasında yoxlama proqramlarının tərtib olunmasına əsaslanır. Test prosesində təhlükəsizlik mexanizmlərinin mövcudluğu və iş qabiliyyəti, sistemin tərkibinin və konfiqurasiyasının təhlükəsizlik tələblərinə və mövcud risklərə uyğunluğu yoxlanılır. Sistemdə zəif yerlərin olması istifadə edilən qoruma vasitələrinin və sistem proqram təminatının konfiqurasiyasının təhlili əsasında aparılır. Bu halda təhlil vasitəsi qismində sistem səviyyəsində qorumanın təhlili üçün reallaşdırılan proqram agentləri istifadə olunur.

Bu paraqrafda informasiya təhlükəsizliyi sisteminin davamlılığının testləşdirilməsi və qiymətləndirilməsi üçün əməliyyat sistemi və şəbəkə xidmətləri səviyyəsində əhəmiyyətli və geniş yayılmış instrumental vasitələr baxılır.

Əməliyyat sistemlərinin qorunmasının təhlili vasitələri

Əməliyyat sistemlərinin qorunmasının təhlili vasitələri əməliyyat sisteminin girişin məhdudlaşdırılması altsisteminin, identifikasiya və autentifikasiya mexanizmlərinin, monitorinq, audit və digər komponentlərinin konfiqurasiyasının sistemin qorunmasının tələb olunan səviyyəsinə uyğunluğunu yoxlamağa imkan verir. Bundan əlavə, bu vasitələr tərəfindən proqram təminatının tamlığına nəzarət, sistem və tətbiqi xidmətlərdə zəif yerlərin mövcudluğunun yoxlanması həyata keçirilir. Əməliyyat sistemlərinin qorunmasının təhlili vasitələrinə nümunə kimi ASET, KSA/KSM, COPS, SSS və s. göstərmək olar.

ASET (Automated Security Tool) - Solaris əməliyyat sisteminin administratorunun proqram təminatına daxil olub, onun təhlükəsizliyinin səviyyəsinin monitorinqi və nəzarət olunması məsələlərini yerinə yetirir. ASET təhlükəsizliyi üç səviyyədə təmin edir: aşağı, orta və yüksək səviyyədə. Təhlükəsizliyin tələb olunan səviyyəsi yüksəldikcə, sistemin qorunmasına daha ciddi tələblər qoyulur.

ASET proqramı əməliyyat sisteminin təhlükəsizliyinin səviyyəsinin monitorinqi və idarə olunması üzrə yeddi əsas məsələni yerinə yetirir:

- giriş atributlarını və sistem fayllarının istifadəsini yoxlayır;
- sistem fayllarının onların təhlükəsizlik şablonlarındakı təsvirlərinə uyğunluğunu yoxlayır;
- istifadəçilərin və qrupların büdcəsini təftiş edir;
- sistemin konfiqurasiya fayllarını təhlil edir;
- dəyişən mühiti nəzarətdə saxlayır;

- aşağı səviyyəli eeprom konfiqurasiyasının qorunması səviyyəsini təmin edir;
- sistemin şəbəkələrarası ekran qismində istifadəsi zamanı qorunma səviyyəsini təmin edir.

Hər bir məsələ üçün spesifik yoxlamalar aparılır və dəyişdirmələr yerinə yetirilir, eləcə də aşkar olunmuş zəifliklər və sistem fayllarında aparılmış dəyişikliklər barədə hesabatlar hazırlanır.

COPS (Computer Oracle and Password System) proqramlar paketi UNIX sistemini təhlükəsizlik administratoru vasitəsi olub, SunOS, FreeBSD, IRIX, AIX, 4.3BSD, Ultrix, HP-Unix, NeXT və digər əməliyyat sistemlərində zəif yerlərin aşkarlanması üçün nəzərdə tutulmuşdur. COPS paketi sistemin testləşdirilməsi zamanı aşağıdakı yoxlamaları yerinə yetirir:

- fayllara, kataloqlara və qurğulara giriş atributları;
- lüğətlər istifadə etməklə seçmə üsulu ilə parolların etibarlılığı;
- istifadəçilərin parollarının və qruplarının faylları;
- istifadəçinin identifikatorunun dəyişdirilməsi atributlarını saxlayan fayllar;
- sistem proqramların yerinə yetirilən kodlarının tamlığı;
- istifadəçilərin ev (ilkin) kataloqlarına və başlanğıc fayllarına giriş hüquqları;
- FTP protokolu üzrə daxil olma konfiqurasiyası;
- poçt xidmətinin konfiqurasiyası;
- servis xidmətlərinin mövcudluğu;
- NFS protokolunun konfiqurasiyası;
- uzaq məsafədə olan sistemlərlə etibarlılıq münasibətlərinin mövcudluğu;

- CERT təşkilatının təhlükəsizlik üzrə materialları ilə tanışolma tarixləri;
- sistemin etibarlılığının itməsinin (nüfuzdan salınmasının) mümkünlüyü.

COPS sisteminin işinin nəticəsi mətn faylı şəklində təqdim olunan və avtomatik olaraq (məsələn, elektron poçtu ilə) aidiyyəti ünvana göndərilən hesabatdan ibarətdir.

SSS (System Security Scanner) sistemi Solaris 2x, SunOS 4.1x, Linux 1.2/1.3, AIX 3.2.5, HP-UX 9.05, 10x(beta) əməliyyat sistemlərinin təhlükəsizlik dərəcələrinin təhlili, eləcə də təşkilatın təhlükəsizlik siyasətinə uyğun olaraq bu sistemlərin qorunmasının idarə edilməsi üçün istifadə olunur. SSS fayllara giriş hüququna nəzarət, faylların sahiblərinin yoxlanması, şəbəkə xidmətlərinin konfiqurasiyasının təhlili, istifadəçi və sistem büdcələrinin qurulması işlərini həyata keçirir.

Bununla yanaşı, SSS sistemdə proqram qoyuluşlarının mövcudluğunun və ziyankarların sistemə digər şəkildə soxulmalarının mümkünlüyünü tədqiq edir. SSS təhlilin nəticələri barədə hesabatda aşkar olunmuş zəif yerləri dəqiq təsvir edir və onların aradan qaldırılması üzrə administratora müvafiq tövsiyələr verir.

SSS sistemi UNIX tipli əməliyyat sistemlərinin zəif yerlərin araşdırılması məqsədilə hər tərəfli testləşdirilməsi imkanlarını təqdim edir.

Praktikada əməliyyat sistemlərinin təhlili vasitələri ilə yanaşı şəbəkə xidmətlərinin qorunmasının təhlili vasitələri də geniş istifadə olunur. Burada belə sistemlər qismində SATAN, Netprobe və Internet scanner proqramları baxılır.

SATAN şəbəkə xidmətlərinin qorunmasının təhlili məqsədilə yaradılan ilk proqramlardan biridir. O, yalnız

təhlükəsizlik administratoru üçün alət kimi deyil, eyni zamanda hücumların həyata keçirilməsi üçün avtomatlaşdırılmış vasitə kimi yayılmışdır. SATAN proqramı uzaq məsafədən işləyən sistemlərin testləşdirilməsi üçün universal yanaşmanı reallaşdırır.

Testləşdirmədən əvvəl informasiya təsiri göstərilə biləcək kanallar, sistemin tipinin identifikasiyası və şəbəkə servis xidmətlərinin versiyaları aşkar olunur. Əldə olunmuş məlumatlar informasiya təsirinin göstərilməsi üçün məlum olan müvafiq zəif yerlər haqqında məlumatların verilənlər bazalarından tapılıb götürülməsi üçün istifadə olunur. Bu isə testləşdirmənin effektivliyini təmin etməyə imkan verir. SATAN proqramı indiyədək istifadə olunur.

SATAN proqramının yeni versiyası – SATAN Extensions çox böyük sayda skanlaşdırılan zəifliklər barədə məlumatlar toplusuna malikdir və şəbəkə xidmətlərini daha ciddi təhlil etməyə imkan verir.

Netprobe (Qualix Group firması) proqramı təhlükəsizlik administratoru üçün vasitə olub, şəbəkə xidmətlərinin proqramlarında zəif yerlərin aşkar olunması və onların aradan qaldırılması üzrə tövsiyələrin verilməsi üçün nəzərdə tutulmuşdur. Zəif yerlərin aşkar olunması mexanizmlərində ziyankarlar tərəfindən uzaq məsafədə olan sistemlərə informasiya təsiri göstərmək üçün tətbiq olunan üsullardan istifadə olunur. Netprobe aşağıdakı imkanları təqdim edir:

- şəbəkə xidmətlərində zəif yerlərin aşkar olunması,
- identifikasiyası və aradan qaldırılması;
- şəbəkələrarası ekranlarda və digər qoruma vasitələrində zəif yerlərin qiymətləndirilməsi;
- informasiya təhlükəsizliyinin tələb olunan

səviyyəsinin təmin edilməsi üzrə tövsiyələrin verilməsi.

Netprobe proqramı şəbəkəyə qoşulmuş Solaris 1.x ƏS idarəsi altında işləyən SunSPARC işçi stansiyası üçün nəzərdə tutulmuşdur.

Zəif yerlərin axtarışı Netprobe proqramı tərəfindən dəstəklənən verilənlər bazasına əsaslanır. Bu verilənlər bazası şəbəkə servis proqramlarında rast gəlinən geniş yayılmış zəifliklər barədə məlumatları özündə saxlayır.

Netprobe proqramı bu bazanı daim yeniləşdirir və aşağıdakıları bazaya daxil etməyə imkan verir:

- yeni zəif yerlər barədə məlumatları;
- zəif yerlərə xidmət edən sorğular toplusunu;
- zəif yerlərin aradan qaldırılması üzrə tövsiyələri.

Netprobe proqramı şəbəkə servislərinin qorunmasının təhlilinin nəticələri üzrə ətraflı hesabat hazırlayır. Bu hesabata aşkar olunmuş zəif yerlərin siyahısını, mümkün təhlükələrin təsvirini və onların aradan qaldırılması üzrə tövsiyələri daxil edir. Hesabatlar mətn və ya hipermətn formatlarında yaradıla bilər.

Internet Scanner (Internet Security Systems Inc. firması) kompüter şəbəkələrinin daxili və xarici hücum- lardan qorunmasının qiymətləndirilməsi üçün nəzərdə tutulmuşdur. Internet Scanner proqramı öz fəaliyyətində informasiya sistemlərinin yüzdən artıq müxtəlif zəiflik-lərinin (zəif yerlərinin) təsvirini, eləcə də təhlükəsizlik problemlərinin mümkün həlli yollarını özündə saxlayan kitabxanadan istifadə edir.

Internet Scanner proqramı daxili şəbəkədə olan bütün serverlərin və işçi stansiyaların testləşdirilməsini təmin edir. O, e-mail, FTP, Network File System və NNTP

xidmətlərinə münasibətdə təhlükəsizlik sistemlərində rast gəlinən 140-dan çox zəifliklərinin mövcud olub-olmamasının yoxlanmasını həyata keçirir. Məsələn, Internet Scanner proqramı şəbəkənin bütün daxili FTP serverlərinə anonim girişin mümkünlüyünü yoxlayır və belə imkanın mövcud olması barədə sistemin administratoruna məlumat verir. Bu proqram, həmçinin, "parolun seçilməsi" (Brute Force) və "xidmətin rədd edilməsi" (Denial of Services) kimi hücumların həyata keçirilməsi imkanlarına malikdir.

§4. Kompüter sistem və şəbəkələrində informasiyanın qorunması üçün proqram-texniki vasitələr

Müasir lokal, korporativ və qlobal informasiya sistemləri xarici resurslara girişin əldə olunması və daxili resursların kənar istifadəçilərə təqdim edilməsi ümumi təyinatlı kompüter sistemlərində və şəbəkələrində (Bundan sonra KSŞ) ərazicə paylanmış hissələri (seqmentləri) arasında qarşılıqlı fəaliyyətin qurulması və informasiya mübadiləsinin həyata keçirilməsi vasitəsilə reallaşdırılır.

Bu zaman kənar istifadəçilər tərəfindən KSŞ-də olan informasiya resurslarına giriş və şəbəkədaxili istifadəçilərin xarici açıq kompüter şəbəkələrinin

resurslarına çıxış imkanlarının təmin edilməsi zərurəti yaranır ki, bu da xarici aləmlə informasiya mübadiləsinin nəzarətdə saxlanılması və korporativ informasiya sistemlərinin, onun qorunan resurslarının kənardan baş verə biləcək mümkün təhlükələrdən qorunması məsələsini çox ciddi şəkildə qoyur.

Qorunan KSŞ-nin resurslarına girişin məhdudlaşdırılması və bu şəbəkə ilə xarici şəbəkələr arasında, elecə də şəbəkənin seqmentləri arasında informasiya axınlarına nəzarət edilməsi üçün bir sıra müasir qoruma texnologiyalardan istifadə olunur. Bu texnologiyalar son dövrlərdə istehsal olunan aparat vasitələrinin, reallaşdırılan proqram vasitələrinin, eləcə də aparat-proqram komplekslərinin tətbiqini nəzərdə tutur.

İnformasiyanın qorunmasının müasir texnologiyalarına əsasən aşağıdakıları aid edirlər:

- şəbəkələrarası qoruyucu ekranlar (brandmauer, fire-
- wall);
- hücumların aşkarlanması sistemləri;
- virtual xüsusi şəbəkələr.

Şəbəkələrarası qoruyucu ekran

KSŞ-nin və ayrı-ayrı kompüterlərin xarici mühit tərəfdən baş verən icazəsiz hərəkətlərdən qorunması üçün, adətən, ikitərəfli məlumat axınının süzgəcdən keçirilməsi və məlumat mübadiləsi zamanı vasitəçiliyin təmin edilməsi funksiyalarını yerinə yetirən şəbəkələrarası qoruyucu ekranlardan istifadə edirlər. Onları çox vaxt qısaca şəbəkə ekranları adlandırırlar.

Şəbəkələrarası qoruyucu ekran (ŞE) – KSŞ-də açıq sistemlərin qarşılıqlı əlaqə (OSI) modelinin müxtəlif

səviyyələrində reallaşdırılan, KSŞ-yə daxil olan və ya KSŞ-dən çıxan informasiya axınlarına nəzarət edən və onları verilmiş qaydalara uyğun olaraq süzgəcdən keçirən lokal və ya funksional baxımdan paylanmış proqram, aparat və ya proqram-aparat vasitələri kompleksidir. ŞE-nin əsas funksiyası KSŞ-ni, onun ayrı-ayrı hissələrini (seqmentlərini) və ya qovşaqlarını icazəsiz girişdən və ya müdaxilədən qorumaqdan ibarətdir.

ŞE onun rəsmi qəbul edilmiş adıdır. Ədəbiyyatlarda eyni zamanda "brandmauer" və "firewall" adlarından da istifadə edilir.

Brandmauer – alman dilində "brand" (yanğın) və "mauer" (divar) sözlərindən ibarət olub "yanğınadavamlı divar" (binalarda yanğının yayılmasının qarşısının alan divar) mənasını verir.

Firewall – sözü isə ingilis dilində "fire" (alov) və "wall" (divar) sözlərindən əmələ gəlmişdir, "yanğın divarı" mənasını verir.

Şəbəkənin konfiqurasiyasında müəyyən edilmiş kriterilərə cavab verməyən paketlərin şəbəkəyə buraxılmaması (süzgəcdən keçirilməsi) funksiyasını yerinə yetirdiyindən onları bəzən ***süzgəc (filtr)*** adlandırırlar.

ŞE-ni, bir qayda olaraq, şəbəkələrin açıq şəbəkəyə, o cümlədən İnternetə qoşulma nöqtəsində yerləşdirirlər. Açıq şəbəkəyə qoşulmuş ayrıca kompüterin qorunması üçün ŞE-nin proqram təminatı həmin kompüterdə quraşdırılır. Belə ŞE-yə ona fərdi ŞE deyirlər.

Göründüyü kimi, ŞE iki şəbəkənin (daxili və xarici şəbəkələrin) sərhəddində nəzarət məntəqəsi rolunda çıxış edir. ŞE təşkilatda qəbul edilmiş informasiya təhlükəsizliyi siyasətinə uyğun olaraq, şəbəkələrarası informasiya

mübadiləsi zamanı təşkilatın KSŞ-nin daxili informasiya fəzasının şəbəkə kənarından baş verə biləcək mümkün hücumlardan qorunması üçün tətbiq edilir. ŞE kənardan daxili şəbəkəyə və daxili şəbəkədən xaricə axan bütün trafikə nəzarət edir (şək.1.1).

Bu məqsədlə ŞE şəbəkənin informasiya resurslarına kənardan girişi məhdudlaşdırmağa imkan verir, təşkilatın qorunan şəbəkəsi, onun informasiya resursları ilə xarici şəbəkə arasında, eləcə də KSŞ-nin hissələri arasında həyata keçirilən bütün informasiya axınlarına nəzarəti təmin edir.

İnformasiya axınına nəzarət onun süzgəcdən (filtrdən) keçirilməsindən və verilmiş qaydalar toplusuna uyğun çevrilməsindən ibarətdir. Müasir ŞE vasitəsilə KSŞ-də informasiya axınının OSI modelinin müxtəlif səviyyələrində süzgəcdən keçirilməsinin mümkünlüyünü nəzərə alaraq, ŞE-ni bəzən süzgəclər sistemi şəklində təqdim edirlər. Bu zaman ardıcıl şəkildə işləyən hər bir süzgəc ŞE ondan keçən məlumatların təhlili əsasında aşağıdakı qərarlardan birini qəbul edir:

- məlumatın keçməsinə icazə vermək;
- ŞE-nin arxasına atmaq;
- məlumatı bloklamaq (dayandırmaq);
- məlumatı çevirmək.

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi üzrə ŞE-nin əsas funksiyaları aşağıdakılardır:

- informasiya mübadiləsi zamanı OSI modelinin kanal, şəbəkə, nəqliyyat və tətbiqi səviyyələrində şəbəkəyə daxil olan (şəbəkədən çıxan) informasiya axınına nəzarət etmək;
- şəbəkə trafikinin kənar şəxslər tərəfindən qulaq

asılmasından qorunması üçün istifadəçiləri identifikasiya və autentifikasiya etmək;
- şəbəkə ünvanlarının translyasiyasını və qorunan şəbəkənin strukturunun gizli saxlanılmasını təmin etmək;
- şəbəkə xidmətlərinə icazəli girişləri təmin etmək;
- resurslara giriş üçün verilən sorğuların və bu sorğuların yerinə yetirilməsinin nəticələrinin qeydiyyatını aparmaq;
- informasiya mübadiləsini protokollaşdırmaq;
- informasiya təhlükəsizliyi siyasətinin pozulması hallarını vaxtında aşkarlamaq və onlara reaksiya verməkdir.

Qeyd etmək lazımdır ki, ŞE-nin ən vacib funksiyalarından biri informasiya mübadiləsinin qeydiyyat jurnalında protokollaşdırılmasından ibarətdir. Belə ki, informasiya axınının protokollaşdırması şəbəkə və ya təhlükəsizlik inzibatçısına şübhəli hərəkətləri, ŞE-nin konfiqurasiyasında olan səhvləri aşkarlamağa və ŞE-nin qaydalarının dəyişdirilməsi haqqında qərar qəbul etməyə imkan verir.

Funksional xarakteristikalarından asılı olaraq, ŞE-ləri aşağıdakı növləri fərqləndirilir:

a) qoşulmaya *görə*
- iki və ya daha çox şəbəkə arasında birləşməni təmin edir;
- hər hansı qovşaqla şəbəkə arasında birləşməni təmin edir.

b) OSI modelinin səviyyəsinə görə
- məlumat axınına OSI modelinin şəbəkə səviyyəsində
- nəzarət edir;

- məlumat axınına OSI modelinin şəbəkə səviyyəsindən
- yuxarı səviyyələrdə nəzarət edir.

c) qoşulmaların izlənməsinə görə

- sadə süzgəc (stateless) – cari qoşulmaları (məsələn, TCP) izlənilmir, məlumat axınını yalnız statistik qaydalar əsasında süzgəcdən keçirir;
- məzmun nəzərə alınmaqla süzgəc (stateful, stateful packet inspection – SPI) – bütün cari qoşulmalar izlənilir, yalnız müvafiq protokolların və proqram əlavələrinin məntiqini və alqoritmlərini ödəyən paketlər buraxılır. Bu növ ŞE müxtəlif növ DoS hücumlara və bəzi şəbəkə protokollarının sındırılmasına qarşı effektiv mübarizə aparmağa imkan verir. Bundan əlavə, statistik qaydalarla pis təsvir olunan ünvanlar arasında məlumatların ötürülməsinin mürəkkəb sxemlərini istifadə edən H.323, SIP, FTP və s. protokolların fəaliyyətini təmin edir.

Nəzarət olunan məlumat axınlarının əhatə dairəsindən asılı olaraq, ŞE-lər iki növə bölünür:

- Ənənəvi ŞE – qoşulmuş şəbəkələr arasında daxil olan və çıxan məlumat axınına nəzarət edən, şlüzdə (şəbəkələr arasında trafiki ötürən serverdə) quraşdı- rılan proqram təminatı (və ya əməliyyat sisteminin ayrılmaz hissəsi) və ya aparat vasitələridir.

- Fərdi ŞE – istifadəçi kompüterində quraşdırılmış və yalnız həmin kompüteri icazəsiz girişdən qorumaq üçün nəzərdə tutulmuş proqramdır.

Xüsusi hada ənənəvi ŞE server tərəfindən özünün resurslarına girişi məhdudlaşdırmaq üçün istifadə olunur.

OSİ modelinin hansı səviyyəsində girişə nəzarətin

həyata keçirilməsindən asılı olaraq, ŞE-ləri aşağıdakı kimi təsnif edirlər :

- körpü tipli ŞE (OSI modelinin 2-ci səviyyəsi); paketləri süzgəcdən keçirən ŞE (OSI modelinin 3-cü və 4-cü səviyyələri);
- seans səviyyəsinin şlüzləri (OSI modelinin 5-cisəviyyəsi);
- tətbiqi səviyyənin şlüzləri (OSI modelinin 7-ci səviyyəsi);
- kompleks ekranlar (OSI modelinin 3-7-ci səviyyələri).

Körpü tipli ŞE (Bridge firewall). Bu növ ŞE-yə bəzən şəffaf, gizli və kölgə ŞE deyirlər. Bu növ ŞE-lər nisbətən yaxın zamanlarda meydana gəlmişdir və onlar şəbəkələrarası ekranlaşdırma texnologiyasının daha perspektivli istiqaməti hesab olunur. OSI modelinin ikinci (kanal) səviyyəsində reallaşdırılan körpü tipli ŞE həmin səviyyədə trafiki süzgəcdən keçirir, ona görə də freymlərlə (kadrlarla) işləyir.

Körpü tipli ŞE-nin üstün cəhətlərinə aşağıdakıları aid etmək olar:

- *Sadəlik*. Onların tətbiqi zamanı KSŞ-nin mövcud parametrlərinin dəyişdirilməsi və ŞE-nin şəbəkə interfeyslərinin yenidən (əlavə) konfiqurasiya edilməsi tələb olunmur;

- *Yüksək səmərəlilik*. Körpü tipli ŞE sadə qurğulardan ibarət olduğuna görə böyük resurs sərfi tələb olunmur. Resurslar yalnız ya sistemin səmərəliliyini yüksəltmək, ya da məlumatları daha dərindən təhlil etmək üçün tələb olunur.

- *Şəffaflıq*. OSI modelinin ikinci səviyyəsində fəaliy-yət göstərdiyinə görə onların şəbəkə interfeysi IP-

ünvana malik olmur. IP-ünvanı olmadığına görə onun sazlanması asan həyata keçirilir və şəbəkədə kənardan görünməz olur. Ona görə də bu növ ŞE-yə hücum etmək mümkün olmur. Belə ki, şəbəkəyə hücumu həyata keçirənlər onların göndərdiyi və aldığı hər bir paketi yoxlayan belə ŞE-nin mövcud olduğunu belə bilmirlər.

Paketləri süzgəcdən keçirən ŞE (Packet-filtering firewall). Bu ŞE, bazasında şəbəkəyə daxil olan və şəbəkədən çıxan paketlərin müəyyən edilmiş növlərini süzgəcdən keçirmək qabiliyyətinə malik olan proqram təminatı quraşdırılmış marşrutlayıcı və ya kompüterdən ibarətdir. Ona görə də onlara ***filtrləyici (ekranlaşdırıcı) marşrutizator*** da deyirlər. Bu növ ŞE-lər OSI modelinin üçüncü və dördüncü səviyyəsində reallaşdırılır.

Pakelər onların TCI və IP başlıqlarında olan informasiya (göndərən və alanın ünvanları, portlarının nömrələri və s.) əsasında süzgəcdən keçirilir. Başqa sözlə, hər bir paket göndərən və alanın ünvanlarından, portlarının nömrələrindən ibarət olan qaydalar siyahısı ilə müqayisə edilir. Bu baxımdan bəzən onları port əsasında işləyən ŞE adlandırırlar.

Onların üstün cəhətlərinə çox ucuz, sürətli və daha az təhlükəli olmasını aid etmək olar.

Seans səviyyəsinin şlüzü (Circuit-level gateway). Seans səviyyəsinin şlüzü icazəli müştəri (kliyent) ilə xarici host arasında birbaşa qarşılıqlı əlaqənin qarşısını alan ŞE-dir. O, əvvəlcə etibarlı müştərinin müəyyən xidmətlər üzrə sorğusunu qəbul edir və tələb edilən seansın mümkünlüyü yoxlanıldıqdan sonra xarici hostla birləşmə yaradılır.

Bundan sonra şlüz hər iki istiqamətə gedən paketləri süzgəcdən keçirmədən onların surətini çıxarır.

Bu səviyyədə ünvanların şəbəkə translyasiyası (NAT – network address translation) funksiyasının istifadə edilməsi imkanı yaranır. Daxili ünvanların translyasiyası şəbəkənin daxilindən xaricinə gedən bütün paketlərə münasibətdə həyata keçirilir. Bu paketlər üçün şəbəkənin daxilində göndərən kompüterlərin IP-ünvanları avtomatik şəkildə ŞE-ni assosiasiya edən hər hansı bir IP-ünvana çevrilir.

Beləliklə, şəbəkədən çıxan bütün paketlər həmin kompüterdən deyil, ŞE-dən göndərilmiş kimi görünür. Nəticədə seans səviyyəsinin şlüzünün IP-ünvanı şəbəkə xaricinə çıxan (kənarda məlum olan) yeganə fəal IP-ünvan olur ki, bu da şəbəkə daxili və şəbəkə xarici kompüterlərin birbaşa əlaqəsini aradan qaldırır.

Seans səviyyəsinin şlüzü, adından göründüyü kimi, OSI modelinin beşinci səviyyəsində işləyir. Porta əsaslanmaqla TCP qoşulmaları ötürür.

Bu ŞE baha deyil, lakin paketləri süzgəcdən keçirən ŞE-yə nisbətən daha təhlükəsizdir. Mükəmməl işləməsi üçün istifadəçinin və ya konfiqurasiya proqramının işləməsini tələb edir.

Tətbiqi səviyyənin şlüzü (Application-level gateways). Daxili şəbəkədən çıxan və xarici şəbəkədən daxil olan bütün paketləri OSI modelinin tətbiqi səviyyəsində süzgəcdən keçirməklə icazəli müştəri ilə xarici host arasında birbaşa qarşılıqlı əlaqəni qarşısını alır.

Tətbiqi səviyyəni şlüzü aşağıdakı imkanlara malikdir:

- ŞE vasitəsilə qoşulmaya cəhd olunan zaman istifadəçilərin identifikasiya və autentifikasiyasının aparılması;
- məlumat paketlərinin süzgəcdən keçirilməsi,

məsələn, virusların dinamik axtarışı, informasiyanın şəffaf şifrlənməsi;
- hadisələrin qeydiyyatı və onlara reaksiyavermə;
- xarici şəbəkədən tələb olunan məlumatların keş yaddaşda saxlanması.

Bu səviyyədə vasitəçilik (Proxy) funksiyasının istifadə edilməsi imkanları yaranır. Tətbiqi səviyyənin xidmət göstərilən hər bir protokolu (FTP, HTTP və s.) üçün vasitəçi proqramları daxil etmək olar. Hər bir TCP/IP xidmətinin vasitəçisi məhz bu xidmətə aid olan məlumatların emalına və qoruma funksiyalarının yerinə yetirilməsinə yönəlmişdir.

Seans səviyyəsinin şlüzünə analoji olaraq, tətbiqi səviyyənini şlüzü daxil olan və çıxan paketləri müvafiq ekranlaşdırıcı agentlərin köməyi ilə tutur, köçürür, şlüz vasitəsilə lazım olan istiqamətə ötürür, daxili və xarici şəbəkələr arasında birbaşa birləşmənin qarşısını alan vasitəçi server qismində fəaliyyət göstərir. Lakin tətbiqi şlüzlər tərəfindən istifadə olunan vasitəçilər seans səviyyəsinin şlüzlərinin vasitəçilərindən mühüm fərqlərə malikdir. Əvvəla, tətbiqi səviyyənin şlüzünün vasitəçisi konkret proqram serverləri ilə bağlı olur. İkincisi, onlar OSI modelinin yalnız tətbiqi səviyyəsində məlumat axınlarını süzgəcdən keçirə bilirlər.

Orta qiymətə malik olan bu şlüzlər daha təhlükəsizdir və istifadəçilərin fəaliyyətinin qeydiyyata almağa imkan verir. Mükəmməl işləməsi üçün istifadəçinin və ya konfiqurasiya proqramının işləməsini tələb edir.

ŞE-lərin qeyd olunan əsas təsnifatından əlavə, təcrübədə aşağıdakı növləri də məlumdur:
- Ekspert səviyyəsinin ŞE (Stateful inspection firewall);

- Fərdi ŞE;
- Dinamik ŞE.

Ekspert səviyyəsinin ŞE – OSI modelinin üç (şəbəkə, seans, tətbiqi) səviyyəsində qəbul olunan paketlərin məzmunlarını yoxlayır. Bunun üçün paketlərin süzgəcdən keçirilməsinin xüsusi alqoritmlərindən istifadə olunur. Bu alqoritmlərin köməyi ilə hər bir paket icazə verilmiş məlum şablonlarla müqayisə olunur.

Fərdi ŞE – hansı növ sistem funksiyalarının və ya proseslərinin şəbəkənin resurslarına girmək hüququna malik olub-olmaması prinsipi əsasında idarəetməyə icazənin verilməsi qoruma imkanlarını daha da genişləndirir. Bu növ ŞE trafikin icazə verilməsi və ya rədd edilməsi üçün müxtəlif növ siqnatura və şərtləri istifadə edə bilər. Məsələn, proqram əlavəsi səviyyəsində bloklama – yalnız bəzi proqram əlavələrinə və kitabxanalara şəbəkə əməliyyatlarını yerinə yetirməyə və ya daxil olan qoşulmaları qəbul etməyə icazə verir; siqnatura əsasında bloklama – şəbəkə trafikini daimi nəzarətdə saxlamağa və bütün məlum hücumların qarşısını almağa imkan verir.

Dinamik ŞE – özündə yuxarıda qeyd olunan standart ŞE-ləri və şəbəkəyə soxulmaların aşkarlanması üsullarını birləşdirir. Dinamik ŞE müəyyən siqnaturalara uyğun gələn şəbəkə qoşulmalarının bloklaşdırılmasını təmin edir və eyni zamanda digər mənbələrdən həmin porta qoşulmalara imkan verir. Məsələn, normal trafikin işini pozmadan şəbəkə qurdlarının fəaliyyətini dayandırmaq mümkün olur.

§5. Şəbəkədaxili girişlərində informasiya təhlükəsizliyinin təmin edilməsi. Şəbəkələrarası qoruyucu ekranların qoşulma prinsipləri

Aydındır ki, KSŞ-nin miqyası nə qədər böyük olarsa, onun təhlükəsizliyinin şəbəkə inzibatçısı tərəfindən etibarlı təmin edilməsi bir o qədər çətin olar. Burada, həmçinin, nəzərə alınmalıdır ki, şəbəkədə icazəsiz girişə və ya müdaxiləyə yalnız işçi stansiyalar, serverlər və ya rabitə xətləri deyil, eyni zamanda məlumat axınlarının şəbəkədaxili marşrutlaşdırma funksiyalarını yerinə yetirən xüsusi qurğular da məruz qala bilər.

Müasir KSŞ-də müxtəlif növ proqram-texniki təminatdan istifadə olunduğuna görə onun mürəkkəbliyi əhəmiyyətli dərəcədə artır. KSŞ-nin qeyri-bircinsliyinin və miq- yasının sürətlə genişlənməsi nəinki şəbəkəxarici, eləcə də şəbəkədaxili xidmətlərdə zəif yerlərin həddən çox artmasına gətirib çıxarır. Belə şəraitdə KSŞ-nin ümumi istifadə olunan resurslarına onun daxili istifadəçiləri tərəfindən icazəsiz giriş və ya müdaxilə təhlükələri də artır.

Bu baxımdan vəziyyətdən çıxış yolu kimi KSŞ-nin ümumi istifadə olunan resurslarının qorunmasını şəbəkə daxili girişin məhdudlaşdırılması səviyyəsini idarə etməklə təmin etmək olar. Bunu isə əvvəlki paraqraflarda qeyd olunan ŞE-nin köməyi ilə reallaşdırmaq mümkündür.

İcazəsiz girişin və müdaxilənin qarşısını almaq üçün ŞE şəbəkədaxili informasiya axınlarının sərhəd nöqtələrində yerləşdirilir. Belə ki, KSŞ-nin ayrı-ayrı seqmentləri, eləcə də istifadəçiləri (kliyentləri) və daha vacib şəbəkə xidmətləri arasında qarşılıqlı əlaqə yalnız ŞE vasitəsilə həyata keçirilir.

Fəaliyyət prinsipinə görə ŞE simmetrik deyildir, yəni onun üçün bir şəbəkə seqmentindən digərinə və əksinə keçidi məhdudlaşdıran qaydalar ayrı-ayrılıqda müəyyən olunur. Ümumi halda, ŞE işi aşağıdakı iki qrup funksiyanın dinamik yerinə yetirilməsinə əsaslanır:

- ondan keçən informasiya axınının süzgəcdən keçirilməsi;
- şəbəkələrarası qarşılıqlı əlaqələrin reallaşdırılması zamanı vasitəçiliyin həyata keçirilməsi.

İnformasiya axınının təhlili üçün kriteri qismində aşağıdakı parametrlərdən istifadə edilə bilər:

- şəbəkə ünvanını, identifikatorları, interfeyslərin ünvanlarını, portların nömrələrini, və digər əhəmiyyətli məlumatları özündə saxlayan məlumat paketlərinin xidməti sahələri;
- məlumat paketlərinin yoxlanılan (məsələn, kompüter virusunun mövcudluğu) məzmunu;
- informasiya axınının xarici xarakteristikaları, məsələn, zaman, tezlik xarakteristikaları, verilənlərin həcmi və s.

Şəbəkələrarası qarşılıqlı əlaqələrin reallaşdırılması zamanı vasitəçilik prosesində ekranlaşdırıcı vasitələr məlumatlar axınının şəffaf ötürülməsini bloklayaraq aşağıdakı funksiyaları yerinə yetirirlər:

- istifadəçilərin identifikasiyası və antentifikasiyası;
- ötürülən məlumatların həqiqiliyinin yoxlanılması;
- qorunan şəbəkə seqmentinin resurslarına girişin məhdudlaşdırılması;
- məlumat axınının filtrasiyası və çevrilməsi, məsələn, virusların dinamik axtarışı və informasiyanın şəffaf şifrlənməsi;

- şəbəkədən və ya onun seqmentindən çıxan paketlər üçün daxili qovşaq ünvanlarının translyasiyası;
- hadisələrin qeydiyyata alınması, onlara reaksiya verilməsi, qeydiyyata alınmış informasiyanın təhlili və hesabatların hazırlanması;
- soruşulan məlumatların keş yaddaşda saxlanması.

Şəbəkələrarası qarşılıqlı əlaqənin qorunmasının effektivliyini təmin etmək üçün ŞE-nin düzgün quraşdırılmasına və konfiqurasiya edilməsinə xüsusi diqqət verilməlidir. Bu proses aşağıdakı mərhələləri ardıcıl yerinə yetirməklə həyata keçirilir:

- şəbəkələrarası qarşılıqlı əlaqə siyasətinin işlənilməsi;
- şəbəkə qurğularının, o cümlədən ŞE-nin qoşulması sxemlərinin müəyyən edilməsi;
- ŞE-nin parametrlərinin köklənməsi.

Şəbəkələrarası qarşılıqlı əlaqə siyasəti təşkilatın təhlükəsizlik siyasətinin onun xarici mühitlə informasiya mübadiləsinin təhlükəsizliyi üçün tələbləri müəyyən edən hissəsi olub aşağıdakı iki aspekti müəyyən edir:

- şəbəkə servislərinə giriş siyasəti;
- ŞE-nin iş siyasəti.

ŞE-nin iş siyasəti onun fəaliyyətinin əsasını təşkil edən şəbəkələrarası qarşılıqlı əlaqənin idarə edilməsinin baza prinsiplərini müəyyən edir. Burada iki prinsipial yanaşma reallaşdırılır:

- açıq icazə verilməyən hər şey qadağan edilmişdir;
- açıq qadağan edilməyən hər şeyə icazə verilmişdir.

Burada qorunan açıq altşəbəkə ekranlaşdırıcı altşəbəkə qismində çıxış edir. Adətən, ekranlaşdırıcı altşəbəkənin konfiqurasiyası elə qurulur ki, altşəbəkənin kompüterlərinə, potensial olaraq, həm xarici şəbəkədən,

həm də lokal şəbəkənin bağlı altşəbəkələrindən daxilolma təmin edilsin, lakin xarici şəbəkə və bağlı altşəbəkələr arasında birbaşa informasiya mübadiləsi mümkün olmasın.

Ekranlaşdırıcı altşəbəkəsi olan sistemə hücum etmək üçün heç olmasa bir-birindən asılı olmayan iki qoruma səddi dəf edilməlidir ki, bu da sındırılma məsələsini çox çətinləşdirir. Bu halda ŞE-nin vəziyyətlərinin monitorinqi vasitələri bütün belə cəhdləri, praktiki olaraq, aşkar etmək və sistemin inzibatçısı isə icazəsiz girişin qarşısının alınması üçün zəruri tədbirlər görmək imkanına malik olur.

Şəbəkələrarası qoruyucu ekranların qoşulma prinsipləri

Kompüter şəbəkələrinə ŞE-nin qoşulması üçün müxtəlif sxemdən istifadə oluna bilər. Bu sxemlər fəaliyyət şəraitindən və ŞE-nin şəbəkə interfeyslərinin sayından asılıdır. Böyük olmayan KSŞ-lər üçün və ŞE-nin istifadəsi kifayətdir.

Burada ŞE-nin şəbəkələrə qoşulması üçün əsas üç sxemdən istifadə olunur:

- lokal şəbəkənin vahid ŞE ilə qorunması sxemi;
- qorunan bağlı və qorunmayan açıq altşəbəkələr sxemi;
- bağlı və açıq şəbəkələrin ayrı-ayrılıqda qorunması sxemi.

Lokal şəbəkənin vahid ŞE ilə qorunması sxemi. ŞE-nin tətbiqinin daha sadə variantı lokal şəbəkə ilə qlobal şəbəkə arasında müvafiq qoruyucu ekranın yaradılmasından ibarətdir.

Belə qoşulma zamanı WWW, FTP, poçt və digər serverlər ŞE vasitəsilə qorunmuş olurlar. Burada əsas diqqətin WWW-serverlər vasitəsilə lokal şəbəkənin qorunan işçi stansiyalarına daxilolmaların qarşısının

alınmasına yönəldilməsi tələb olunur.

Qorunan bağlı və qorunmayan açıq altşəbəkələr sxemi. Bu sxemdə WWW serverin resurslarından istifadə etməklə lokal şəbəkəyə girişin qarşısını almaq məqsədilə ümumi girişli serverlərin ŞE-dən qabaqda yerləşdirilməsi Bu üsul lokal şəbəkənin daha yüksək qoruması səviyyəsini təmin edir, lakin bu zaman WWW, FTP və poçt serverlərinin qorunma səviyyəsi aşağı olur.

Bağlı və açıq şəbəkələrin ayrı-ayrılıqda qorunması sxemi. Bu sxem əvvəlki qoşulmalarla müqayisədə ən yüksək qorumanı təmin edir. Sxem bağlı və açıq altşəbəkələri ayrı-ayrılıqda qoruyan iki ŞE-nin tətəbiqinə əsaslanır.

Şəbəkənin ŞE-ləri arasında qalan hissəsi ekranlaşdırılmış altşəbəkə və ya demilitarizasiya edilmiş zona adlanır.

Hücumların aşkarlanması sistemləri

KSŞ-nin, eləcə də onun bazasında fəaliyyət göstərən korporativ informasiya sistemlərinin normal işinin təmin edilməsi məqsədilə şəbəkə hücumlarının qarşısının alınması üçün standart qoruma vasitələri (məsələn, ŞE, ehtiyat surətin saxlanılması sistemi, antivirus proqramları) ilə yanaşı reallaşdırılması zəruri olan əsas vasitələrdən biri də hücumların aşkarlanması sistemləridir.

Müasir dövrdə hücumların aşkarlanması sistemləri (HAS) KSŞ-lərin təhlükəsizliyinin təmin edilməsi təcrübəsində getdikcə daha geniş tətbiq olunur. Lakin şəbəkə- lərdə HAS-ı reallaşdıran və istifadə edən təşkilatlar onun tətbiqi prosesini əhəmiyyətli dərəcədə çətinləşdirən, hətta dayanmasına səbəb olan bir sıra ciddi problemlərlə mütləq üzləşirlər. Bu problemlərə

aşağıdakıları aid etmək olar:

- kommersiya əsaslı HAS-ın qiymətinin yüksək olması;
- müasir HAS-ın səhvən işə düşmə və ya düşməmə hallarının sayının böyüklüyü ilə xarakterizə olunan effektivliyinin yüksək olmaması;
- şəbəkə resurslarına yüksək tələbatın, bəzən isə hətta 100 Mbit/san sürətində qeyri-kafi məhsuldarlığın olması;
- şəbəkə hücumlarının həyata keçirilməsi ilə bağlı
- risklərin kifayət qədər qiymətləndirilməməsi;
- təşkilatda riskin qiymətini adekvat müəyyənləşdirməyə və əks-tədbirlərin reallaşdırılmasının qiymətini rəhbərlik üçün əsaslandırmağa imkan verən risklərin təhlili və idarə edilməsi metodikasının olmaması;
- HAS-ın tətbiqi və genişləndirilməsi ilə məşğul olan ekspertlərin hücumların aşkarlanması üzrə ixtisas dərəcələrinin kifayət qədər yüksək olmaması.

Azərbaycan Respublikası üçün təşkilatlarda informasiya infrastrukturunun İnternetdən nisbətən az asılı olması və informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlərin zəif maliyyələşdirilməsi xarakterikdir ki, bu da şəbəkə hücumlarının qarşısının alınması üçün bahalı qoruma vasitələrinin əldə olunmasına imkan vermir. Buna baxmayaraq, respublikamızda da informasiya təhlükəsizliyinin təmin edilməsi üçün HAS getdikcə daha çox istifadə olunur və onun tətbiqi texnologiyası inkişaf edir.

HAS-ın nümunəvi arxitekturasına, bir qayda olaraq, aşağıdakı komponentlər daxil olur:

- informasiyanın toplanması vasitələri – sensor;
- informasiyanın təhlili vasitələri – analizator;

- reaksiyavermə vasitələri;
- idarəetmə vasitələri.

HAS-ın bütün komponentləri bir kompüterdə və ya bir proqram əlavəsi çərçivəsində reallaşdırıla və fəaliyyət göstərə bilər. Lakin onların kompüter şəbəkəsinin qovşaqları üzrə ərazicə və funksional baxımdan paylanması daha məqsədəuyğun hesab olunur.

HAS-ın analizator və idarəetmə vasitələrinin ŞE-dən sonra xarici şəbəkədə yerləşdirilməsi çox təhlükəlidir. Belə ki, əgər bu vasitələr sındırılarsa, onda bədniyyətli şəxs HAS-da istifadə olunan baza qaydalarını təhlil etməklə qorunan daxili şəbəkənin strukturu haqqında məlumatlara giriş əldə edə bilər.

Host sensorları informasiya mənbəyi qismində əməliyyat sisteminin, verilənlər bazasının idarə edilməsi sistemlərinin və proqram əlavələrinin hadisələrin qeydiyyatı jurnalından istifadə edirlər. Hadisələr haqqında məlumatlar, həmçinin host sensoru tərəfindən bilavasitə əməliyyat sisteminin özəyindən, ŞE-dən və ya proqram əlavəsindən alına bilər.

Təhlükəsizlik serverində yerləşən analizator sensorlardan alınan məlumatların mərkəzləşdirilmiş qaydada yığılması və təhlilini həyata keçirir.

HAS-ın reaksiyavermə vasitələri şəbəkənin monitorinqini həyata keçirən kompüterlərdə, ŞE-də, serverlərdə və lokal şəbəkələrin işçi stansiyalarında yerləşdirilə bilərlər.

Hücumlara reaksiyavermə üzrə hərəkətlərin nümunəvi toplusu təhlükəsizlik inzibatçısının xəbərdar edilməsi (elektron poçtu vasitəsilə, məlumatı konsola çıxarmaq və ya peycerə göndərmək yolu ilə), hücumların qarşısının dərhal alınması məqsədilə şəbəkə seansının və ya istifa-

dəçilərin qeydiyyatı prosesinin dayandırılması, eləcə də hücum edənin hərəkətlərinin protokollaşdırılması kimi hərəkətləri özündə birləşdirir.

İdarəetmə vasitələri HAS-ın bütün komponentlərinin idarə olunması, təhlükəsizliyin (təhlükəsizlik siyasətinin) pozulması hallarının aşkarlanması və onlara reaksiya verilməsi alqoritmlərinin işə salınması, eləcə də pozulmalar haqqında məlumatların baxılması və hesabatların hazırlanması üçün nəzərdə tutulmuşdur.

§6. Şəbəkə daxilindən və şəbəkə xaricindən olunan hücumlarlardan qorunma yolları.

İnformasiya sistemlərində kiber hücumlara və təhdidlərə qarşı təhlükəsizliyi önəmli olan sistemlərdən biri də şəbəkə sistemləridir.

Şəbəkə sistemlərinə iki növ şəbəkə hücumları baş verir.

Şəbəkə daxilindən və şəbəkə xaricindən olunan hücumlar.

Şəbəkələrimizi kənar hücumlardan qoruyan zaman şəbəkəni Firewallsız (Güvənlik divarı) təsəvvür etmək mümkün deyil. Firewallar daxili şəbəkəmiz ilə xarici şəbəkə arasında axan trafiki yoxlayır, təyin etdiyimiz policylərə görə məhdudiyyətlər qoyur, hansı paketlərin firewall üzərindən internetə və ya əksinə hərəkət edəcəyinə qərar verib şəbəkəni kənardan gələn təhdidlərə qarşı qoruyur. Bu

səbəbdən Firewallar, şəbəkənin kənar təhdidlərə qarşı qorunmasında əsas rolu oynayır.

Aşağıda sadaladıqlarımı Firewallarda tətbiq etməklə şəbəkəmizi xarici təhdidlərdən qoruya bilərik. Bunun üçün Firewallda :

- Bütün portları bağlamaq və yalnız lazım olan portları açmaq.
- Policy-lərə portlar ilə paralel olaraq tətbiqlər və istifadəçi adlarını da əlavə etmək.
- Trafikin analiz edilməsi, imza bazasının daim yenilənməsini təmin etmək.
- İş ilə əlaqəli olmayan və zərərli kodlar bulaşdırılmış web səhifələrinə girişləri əngəlləmək.
- Zərərli kod bulaşdırılmış faylların endirilməsini əngəlləmək.
- Firewallda SSL decryption, inspection aktivləşdirmək – gələn və gedən trafiki oxumaq, analiz etmək.
- Tətbiq edilmiş policy-lər ilə birgə security profile-lar istifadə etmək (antivirus, web filtering, email filter, dns filter, anty-spyware və s.)
- Dos atack, Packet based attack, Protocol attack, icmp flood, udp flood kimi hücumların qarşısını almaq üçün tədbirlər görmək (DOS protection, icmp flood protection və s.)
- Mütəmadı olaraq loglar çıxarmaq – şübhəli məqamlarda trafiki incələmək üçün.
- Daxili şəbəkəyə internet üzərindən təhlükəsiz qoşulmaq üçün vpn protokolundan istifadə etmək.

Qabaqlayıcı tədbirlərin əksəriyyəti yeni nəsil Firewallarda mümkündür.

Köhnə nəsil Firewallarla müqayisədə yeni nəsil firewallar icazəsini əngəllədiyimiz internetə çıxışı olan proqramları, portları bütövlükdə əngəlləmir. Yeni nəsil firewallar köhnə nəsil firewallarla müqayisədə daha ağıllı işləyir, application id və content id vasitəsilə tətbiqi yoxlayır, bütünlüklə tətbiqə deyil həmin tətbiqin hər hansı funksiyasını bloklayır.Yəni layer 7 səviyyəsində də işləyir.

Məsələn facebook proqramına icazə verdiyiniz halda istəyinizə uyğun olaraq facebookda hər hansı paylaşım etməyi bloklaya bilərsiniz. Başqa bir misal Facebook web səhifəsinə girişi blokladığınız halda istədiyiniz istifadəçi üçün facebook səhifəsinə girişi açа bilərsiniz. Yuxarıda sadalananları Firewallarda tətbiq etməklə kənardan şəbəkəyə olunan hücumların qarşısını almaq mümkündür.

Şəbəkə hücumlarının ikinci növü daxili şəbəkə hücumlarıdır. Belə ki kiber cinayətkarlar bu hücumları reallaşdırmaq üçün artıq sizinlə eyni şəbəkədə olur. Daxildən şəbəkəyə olunan hücumlar da 2 hissəyə ayrılır. Simli və simsiz şəbəkə hücumları.

Simli şəbəkə hücumlarından qorunmaq üçün aşağıda sadaladığım protokolları və üsulları tətbiq etmək olar.

İlk öncə şəbəkə avadanlıqlarımızda istifadə etmədiyimiz portları (interfeysləri) söndürmək – kiber cinayətkar fiziki yolla hər hansı şəbəkə avadanlığımıza qoşulsa belə həmin port aktiv olmayacaq.

Şəbəkə avadanlıqlarına qoşulma zamanı etibarlı protokollar (ssl, https, ssh) istifadə etmək – telnet və http kimi protokollarla şəbəkə avadanlıqlarına qoşulan zaman şifrəmizi yazanda dinlənməyə məruz qalmışıqsa cinayətkar şifrəmizi görə bilir.

Daxili şəbəkəmizi virtual lanlara ayırmaq – şəbəkəni alt şəbəkələrə ayırmaqla baş verə biləcək riskləri azaltmaq.

Port security protkolu istifadə etmək – hər porta cihazin mac ünvanını statik daxil edib o porta yalnız o cihazın qoşulmasına icazə vermək.

Etibarlı kimlik doğrulama serverləri istifadə etmək – şəbəkə cihazlarımıza giriş üçün əlavə kimlik doğrulama serverinə müraciət ediriksə o server ilə cihazımızın arasındakı traffikin şifrələnmiş olduğuna əmin olmaq.

Dos attacklarına qarşı storm control istifadə etmək – Saniyədə portumuzdan keçən paket sayına müəyyən limitlər qoyub bu hücumların qarşısını ala bilirik.

DHCP snooping istifadə etmək – cihazlar dhcp sorğularını yalnız təyin olunmuş portdan yaxud vlandan göndərir və şəbəkədə saxta dhcp serverlər fəaliyyət göstərə bilmir.

Vlan hopping hücumları – qarşısını almaq üçün interfeysləri auto yaxud dinamik modda buraxamamaq , statik olaraq interfeysin növünü təyin etmək, trunk portlardan bütün vlanları deyil, yalnız bizə lazım olan vlanları göndərmək.

Arp spoofing attack – ortadakı adam hücumu ən geniş yayılmış hücum növüdür, şəbəkə üzərindən gedən paketləri (şifrələnməyibsə) dinləmək olur. Qarşısını almaq üçün statik arp cədvəli təyin etmək , detection tool istifadə etmək, paketləri filterləmək və s.

Access listlər təyin etmək – access list vasitəsilə şəbəkədə olan ip ünvanlarının istəmədiyimiz iplər ilə əlaqə qurmasının qarşısını almaq.

Cihazlara qoşulma üçün 1 ip ünvanı təyin etmək – access list vasitəsilə, yalnız o ip ünvanı cihaza uzaqdan qoşula bilsin.

Kimlik doğrulama dəstəkləyən yönləndirmə (routing) protokolları istifadə etmək (OSPF v3, RİP v2 və s.)

NTP server təyin edib cihazlarımızın vaxt və tarixi eyni cihazdan öyrənməsini təmin etmək.

Göstərilən protokolları və üsulları istifadə etməklə şəbəkəmizin təhlükəsizliyini şəbəkədaxili hücumlardan qoruya bilərik.

Simsiz şəbəkəyə hücumlarının fiziki qoşulma tələb etmədiyini düşünsək, simsiz şəbəkəyə hücumlar təşkil etmək cinayətkarlar üçün daha əlverişlidir. Simsiz şəbəkənin təhlükəsizliyini qorumaq üçün aşağıdakı üsullardan istifadə edə bilərik :

- Düzgün şifrələmə üsulu seçmək – Wep və wpa istifadə etmək çox risklidir. 64 və 128 bitlik şifrələmə istifadə edir, asan qırılır.
- WPA2 şifrələmə növünü AES ilə birlikdə istifadə etmək - Günümüzdə hələdə asanlıqla qırılmır.
- WPA3 şifrələmə növünü istifadə etmək – WPA2-dən fərqli olaraq WPA3 istifadə edən simsiz şəbəkənin şifrəsini tapmaq mümkün deyil. Çünki WPA3 WI-FI Certified Enhanced Open standartı istifadə edir, belə ki siz hətta açıq simsiz şəbəkəyə qoşulan zaman sizin cihaz ilə simsiz şəbəkə cihazı arasında avtomatik güclü şifrələnmə yaranır.
- WPS deaktiv etmək - Cihazımız wpsi dəstəkləyirsə, qoşulan cihaz da wpsi dəstəkləyirsə bu zaman wps düyməsini hər iki cihazda basıb qoşulmanı başlada

bilərik. Əsasən printerlərin şəbəkəyə qoşulması üçün istifadə olunur. Şifrənin tapılması çox asan olur.

- Statik mac ünvanları təyin etmək – simli şəbəkədə olduğu kimi arp spoofing atacklarının qarşısını almaq.
- SSİD gizlətmək – Professional hackerlər üçün gizli ssid-ni tapmaq çox asan olsa da ssid-ni gizlətməkdə fayda var.
- Simsiz şəbəkə cihazının və mərkəzi idarə etmə sisteminin proqram versiyasını son versiyaya yüksəltmək.
- Şirkət daxilində Qonaqlar üçün ayrılmış alt şəbəkə ilə əlavə SSİD istifadə etmək.
- WI-FI kanallarını yoxlamaq - ətrafdakı simsiz şəbəkələri yoxlamaq ən az istifadə olunan WI-FI kanalını istifadə etmək.

Kiber hücumları planlayan cinayətkarlar üçün hücumlarını reallaşdırmağa dəqiq bir üsul yoxdur. Mümkün ola bilən bütün üsulları yoxlayacaqlar. Bu səbəbdən şəbəkəmizi istər kənar hücumlar, istər daxili və simsiz şəbəkə hücumlarından qorumaq üçün ən azı yuxarıda sadalananları tətbiq etmək lazımdır.

Firewall şəbəkənizə daxil olan və çıxan bütün məlumat paketlərinə nəzarət edir. Bu məlumat paketləri şəbəkənizdəki cihazlar arasında əlaqə yaratmaq üçün istifadə olunur. Firewall bu məlumat paketlərini təhlil edir və onları müəyyən qaydalar toplusuna uyğun olaraq filterdən keçirir. Məsələn, daxil olan məlumat paketi müəyyən bir portdan gəlirsə və təhlükəsizlik prinsiplərinə uyğun gəlmirsə, firewall bu paketi bloklayır. Həmçinin daxili şəbəkənizdəki cihazlar tərəfindən göndərilən

məlumat paketlərini yoxlayır və zərərli bir məlumat aşkar etdikdə bloklayaraq təhlükəsizliyi təmin edir.

Firewall növləri

Firewallar vasitəsi ilə təhlükəsizlik məsələləri müxtəlif yollarla həyata keçirilə bilər və firewallın müxtəlif növləri var. Ən çox yayılmış firewall növləri bunlardır:

- Stateless Firewall — Məlumat paketlərini müstəqil idarə edir. Hər bir paketi ayrı-ayrılıqda dəyərləndirir.
- Statefull Firewall — Məlumat paketlərini müstəqil qiymətləndirmək əvəzinə, əvvəlki paketlərin tarixini nəzərə alır. Bu yolla da təhlükəsizliyi artırır və təhlükəli trafikin qarşısını alır.
- Application Layer Firewall — Paketləri yalnız IP ünvanı və ya port məlumatlarına görə deyil, həm də içəriyinə görə filterləyir. Bu, zərərli içəriyi tanımaq və daha dəqiq nəzarət təmin etmək üçün yaxşıdır.

Firewallın önəmi

Firewall internet təhlükəsizliyinin təməlidir və bir çox vacib funksiyaları yerinə yetirir deyə bilərik. Məsələn onlardan bəziləri bunlardır:

- İcazəsiz girişin qarşısının alınması: Firewall icazəsiz girişin qarşısını alaraq şəbəkənizi icazəsiz girişdən qoruyur. Bu, hakerlərin şəbəkənizə sızmasının və həssas məlumatlara çatmasının qarşısını alır.
- Zərərli proqramların bloklanması: Firewall zərərli proqramların şəbəkənizə daxil olmasının qarşısını alır. Viruslar kimi zərərli proqramları aşkar edərək istifadəçiləri qoruyur.
- Məlumatların filtrlənməsi və nəzarəti: Firewall şəbəkənizdən gedən və daxil olan məlumatları

filtrləyərək isdənməyən məzmunun qarşısını alır. Bu, şəbəkə trafikinin nəzarət altında saxlanmasını və hücumlardan qorunmasını təmin edir.

- Təhlükəsizlik prinsiplərinin tətbiqi: Firewall tələkəsizlik prinsiplərini tətbiq edir və bu prinsiplərə uyğun gəlməyən trafiki bloklayır. Məsələn, müəyyən bir ölkədən gələn trafiki bloklamaq və ya müəyyən protokoldan istifadəni qadağan etmək kimi prinsipləri təyin edə bilərsiniz.

§7. Kompüter cinayətkarlığı

Kiber təhlükəsizlik–verilənlərin əlyetənliyinin, bütövlüyünün və konfidensiallığının təmin edilməsi üçün təhlükəsizlik tədbirlərinin istifadə edilməsi prosesləridir. Sistem administrator əsas vəzifəsi lokal şəbəkəmim kompyüterlərinin, serverlərin və aktiv istiofadəçilərin mühafizəsini təmin etməkdir. Kibertəhlükəsizliyiyn məqsədi verilənlərin mühafizəsidir.

Verilənlərin təhlükəsizliyinin təmin edilməsi üçün əks tədbirlər görülə bilər. Bu gün biz qlobal qarşılıqlı əlaqələr dünyasında yaşayırıq. Biz bir an içində dünyanın o biri başındakı insanlarla söhbət edə, yaxud böyük məbləğdə pul əməliyyatları həyata keçirə bilirik. Fərdi komputerlərin sayının görünməmiş surətlə artması, İnternetə sərbəst çıxış və yeni kommunikasiya qurğularının surətli inkişafı həm asudə vaxtın keçirilməsi, həm də biznesin aparılması

üsullarını dəyişdirdi. Eyni zamanda qaraniyyətli insanlar üçün də yeni imkanlar açıldı, yeni cinayət üsulları meydana çıxdı. Bəşəriyyət yeni cinayət növü ilə – kibercinayətkarlıqla qarşılaşdı.

Kibercinayətkarlıq dedikdə, İnternet, yaxud başqa kompüter şəbəkələrindən istifadə olunmaqla törədilən cinayətlər nəzərdə tutulur. ―Kibercinayətkarların‖ hücum obyektləri, əsasən, banklar, birjalar, İnternet-mağazalar olur. Cinayətin həyata keçirilməsində komputerlər, yaxud şəbəkələrdən aşağıdakı kimi istifadə oluna bilər:

- Kompüter, yaxud şəbəkə cinayət aləti ola bilər, başqa sözlə, cinayətin həyata keçirilməsində onlardan istifadə oluna bilər.
- Kompüter, yaxud şəbəkə cinayətin hədəfi (―qurbanı‖) ola bilər.
- Kompüter, yaxud şəbəkə cinayətli məqsədlərə çatmaq üçün yardımçı vasitə ola bilər.

Hakerlər

Komputerlər yenicə meydana çıxanda "haker" sözü hörmətlə çəkilirdi. Əməliyyat sisteminin daha yaxşı işləməsi üçün onun nüvəsinin bir hissəsini yenidən yazan, yaxud hamının unutduğu administrator parolunu ―ləğv edən‖ kompüter dahilərini belə adlandırırdılar. Qeyri-standart düşünmə qabiliyyətlərinə və ən mürəkkəb problemlərin ağıllı həllini tapdıqlarına görə bu, onlara hörmət əlaməti idi. Lakin zaman ötdükcə bu söz əsl mənasını itirdi, çünki ―hakerlərin heç də hamısı öz ənənəvi işləriylə kifayətlənmədilər. Onların bəziləri pis mühafizə olunmuş kompüter sistemlərinə girməyə və bununla da ―bunun mümkünlüyünü sübut etməyə‖ başladılar.

Başqaları isə hər hansı mühüm informasiyanı oğurlamaq məqsədilə sistemləri—sındırmaqla məşğul oldular. Haker termininin öz mənasını itirdiyini görən komputer ictimaiyyəti əlavə terminlər (məsələn, ―script kiddie‖ və -cracker‖) daxil etdilər. "Script kiddie" (ssenari uşağı) termini ilə hakerlik sahəsində o qədər də biliyi olmayan və ―sındırmaq üçün digər hakerlərin utilitlərindən istifadə edən adamları adlandırırlar.

"Cracker" (kreker) isə bilik səviyyəsinə görə "script kiddie" ilə haker arasında olan şəxsə deyilir. O, proqramların üzünün çıxarılmaması üçün qoyulmuş müdafiəni ―sındıra bilir, ancaq proqramda yeni zəif yerlər tapmaq, yaxud haker utilitləri yazmaq üçün onun biliyi kifayət etmir.

Proqram təminatı piratçılığı.

Proqram məhsulunun alıcısı əslində yalnız həmin proqramın istifadə hüququnu əldə edir. Proqramın özü isə onun mülkiyyətinə keçmir. Ona görə də proqram məhsulunun üzünün çıxarılıb yayılması qanun pozuntusu hesab olunur. Belə hərəkətlərə kompüter piratçılığı, yaxud proqram təminatı piratçılığı deyilir.

Kompüter piratçılığı proqram təminatı bazarı üçün çox böyük problemdir. İstifadədə olan hər bir lisenziyalı (qanuni yolla əldə olunmuş) proqrama ən azı bir lisenziyasız, yaxud ―pirat‖ nüsxə düşür. Bəzi ölkələrdə isə bu, 1:9 nisbətinə çatır. Piratçılıq proqram təminatı istehsalına çox mənfi təsir göstərir, yeniliyin qarşısını alır, proqram məhsulunu hazırlayanları və istehsalçıları planlaşdırdıqları gəlirdən məhrum edir. Proqramların üzünün icazəsiz koçürülməsinin qarşısını almaq üçün xüsusi vasitələrdən istifadə oluna bilər.

Lisenziyalı proqramın distributiv dəstinə daxil olan bəzi verilənlər proqramın özünə daxil olmur. Belə proqramın üzü çıxarılarkən həmin verilənlər itə bilər ki, bu da mühafizə üsullarından biridir. Müəlliflik hüququ. İnformasiya-kommunikasiya texnologiyalarının dinamik inkişafı və komputerlərin çox surətlə insanların həyatına daxil olması ilk vaxtlar qanunvericilərin buna hazır olmadığını göstərdi. Bir müddət kompüter proqramlarının hüquqi müdafiəsi məsələsi açıq qaldı.

Lakin getdikcə bu boşluqlar doldurulmağa başlandı. Belə ki, hazırda kompüter proqramları (kompilyatorlar, redaktorlar, verilənlər bazası və s.) əmtəə məhsulu statusu almışdır və onlar da intellektual mülkiyyət kimi qorunur. Kompüter proqramlarının müəlliflik hüququnun tanınması üçün onların hər hansı qurumda qeydiyyatdan keçirilməsi vacib deyil.

Proqrama müəlliflik hüququ avtomatik olaraq onun yaradılması zamanı meydana çıxır. Proqramın yaradıcısı öz hüquqlarını elan etmək üçün proqramın ilk buraxılışında üç elementdən ibarət olan müəlliflik hüququnun qorunması işarəsindən istifadə edə bilər:

- çevrənin icərisində, yaxud mötərizədə ―C‖ hərfi – ©, (C);
- hüquq sahibinin adı;
- proqramın ilk buraxılış ili.

§8. İnformasiya təhlükəsizliyində biometrik parametrlər

Dünyada terror təhlükəsinin artması ilə əlaqədar olaraq təhlükəsizliyi təmin edən sistemlərin təkmilləşdirilməsi məqsədilə biometrik identifikasiya sistemlərinin yaradılması zərurəti meydana çıxmışdır.

İnformasiya texnologiyalarının sürətli inkişafı nəticəsində bir çox yeni vasitə və qurğular həyatımızın bir hissəsinə çevrildi. Cihazların rahatlığına alışmış insanlar tez bir zamanda avtomatlaşdırma sistemlərindən asılı olurlar. Məsələn, bəzi iş yerlərində girişlərdə avtomatik açılan və bağlanan qapılar rahat bir vasitə hesab edilə bilər.

Xüsusilə ölkə sərhədlərini keçəndə təhlükəsizlik elementlərinin xeyli artdığı görülür. Barmaq izlərini götürmək, barmaq izlərini sonrakı girişlərlə müqayisə edərək ölkəyə girməyi asanlaşdırır. Təhlükəsizlik təcrübələri ilə yanaşı, saxta məhsullar da gündəmdədir və bir çox sistem ciddi hücumlara məruz qalır. Bu çərçivədə ağla gələn ilk şey təhlükəsizlik, kart, açar və s. Bu, oğurluq və icazəsiz şifrə mübadiləsi kimi bir çox problemi aradan qaldıran biometrik metodların inkişafına səbəb oldu.

Etibarlı identifikasiya bu gün çox vacibdir. Üç identifikasiya üsulu arasında, yəni bilik bazası identifikasiyası, mənşəli əsaslı autentifikasiya və biometrik əsaslı identifikasiya arasında biometrik eyniləşdirmə ən etibarlı metod kimi tanınır. Tədqiqatçılar yüksək dəqiqliyi təmin etmək üçün tədqiqatlarını yeni biometrik sistemlər üzərində cəmləşdirirlər. Ancaq bu texnologiyanın geniş yayılması üçün xərcləri daha əlverişli etmək lazımdır. Biometrik sistemlərin əhəmiyyəti fərdi xüsusiyyətlərin

inkişaf etdirilməsidir. Xüsusi xüsusiyyətlər, köçürmələrin mümkün olmadığı təqdirdə yüksək təhlükəsizliyi təmin edir. Buna görə, bu xüsusiyyətlərlə biometrik sistemlər pasport nəzarətindən bank əməliyyatlarına qədər geniş tətbiq tapır və vacib bir tədqiqat mövzusu olaraq ortaya çıxır.

Biometrik sistemin əsas üstünlüyü insanların heç yerdə unutmağı və itirməməsini təmin edən bir əza ilə tanıya bilməsidir. Buna görə gələcək üçün planlaşdırılan təhlükəsizlik sistemlərinin əsas məqsədi insanların heç bir kart və ya açar daşımadan və ya şifrələri yadda saxlamadan asanlıqla tanınmasıdır.

Biometrik informasiyaya əsaslanan mühafizə sistemləri də mövcuddur. Bu sistemlərdə istifadə olunan əlamətlər insanın dəyişməyən xususiyyətlərinə əsaslanır və ona görə də biometrik informasiya itirilə, yaxud saxtalaşdırıla bilməz. İnformasiyanın biometric mühafizə sistemlərinə aşağıdakı identifikasiya (şəxsin tanınması) sistemləri aiddir:

a) barmaq izlərinə görə identifikasiya;
b) gözün qüzehli qişasının şəklinə görə identifikasiya;
c) nitqin özəlliklərinə görə identifikasiya;
d) üzün təsvirinə görə identifikasiya;
e) ovucun cizgilərinə görə identifikasiya.

Müxtəlif tətbiqlərdə bir sıra biometrik parametrlər istifadə edilir. Hər biometrik parametrin üstün və zəif cəhətləri var və seçim adətən tətbiqdən asılı olur. Aşağıda geniş məlum olan biometrik parametrlərin qısa xülasəsi verilir.

Barmaq izləri

Barmaq izlərinə görə identifikasiya texnologiyası ən geniş yayılmış biometrik texnologiyadır. Bu metodun əsasında hər bir insanın əl barmaqlarında papilyar naxışların unikallığı ideyası durur.

Barmaq izini papilyar xətlər əmələ gətirir, onların quruluşu dərinin şırımlarla ayrılmış qılıc çıxıntılarının sıraları ilə şərtlənir. Bu xətlər mürəkkəb naxışlar əmələ gətirirlər (qövs, ilgək və spiral), onların aşağıdakı xassələri var:

- fərdilik və təkraredilməzlik;
- zamana görə sabitlik (bətndaxili inkişafdan meyidin çürüməsinədək);
- bərpa olunma (dəri qatının səthi zədələndikdə xətlərin quruluşu əvvəlki şəklində bərpa olunur).

Barmaq izinin tanınması və onun alqoritm tərəfindən düzgün emalının keyfiyyəti barmaq səthinin vəziyyətindən və skaner elementinə nəzərən onun yerləşməsindən çox asılıdır. Müxtəlif sistemlər bu iki parametrə müxtəlif tələblər irəli sürür. Tələblərin xarakteri xüsusi halda tətbiq edilən alqoritmdən asılıdır.

Barmaq izinin identifikasiyası

Barmaq izinə görə identifikasiya-bu ən geniş yayılmış biometrik texnologiyadır. International Biometric Group-un verilənlərinə görə, barmaq izinə görə tanıma sistemləri bütün dünyada istifadə olunan biometrik texnologiyaların 52%-ni təşkil edir. Tanıma üçün barmaq izinin istifadəsinin nə vaxtdan başladığını söyləmək çətindir. Arxeologlar qazıntı zamanı daş üzərində barmaq izlərinin şəkillərinə rast gəlirdilər. Lakin bu heç də onların identifikasiya üçün istifadəsini təsdiqləmir. Digər tərəfdən məlumdur ki,

Qədim Vavilon və Çində gil lövhəciklər və möhürlər üzərində barmaqların şəkillərini düzəldirdirlər. XIV əsrdə Iranda barmaq izi ilə bir sıra dövlət sənədlərini imzalayırdılar. Bu o deməkdir ki, hələ o vaxtlardan barmaq izi insanın nadir xüsusiyyətlərindən biridir ki, ona görə insanı identifikasiya etmək olar.

Texnologiyanın inkişafının növbəti mərhələsi barmaq izinin krimanlda istifadəsi ilə başlandı. XIX əsrin ortalarında hər bir insanın barmaq izlərinin nadirliyi haqqında ilk fərziyyə yarandı və barmağın müxtəlif cizgilərinə görə onların klasifikasiyasına cəhd edildi. Bütün bunlar 1897-ci ildə «Genri sistemi»nin yaranmasına gətirib çıxartdı. Bu sistem barmaq izini klasifikasiyasında geniş yayılmışdır. Sistem ingilis Edvart Genri tərəfindən Hindistana səfəri zamanı yaradılmışdır. XIX əsrin sonlarında barmaq izlərinin ilk müqayisə alqoritmi yaradıldı. Növbəti 25 il ərzində «Genri sistemi» müxtəlif ölkələrdə dövlət səviyyəsində istifadə üçünn uyğunlaşma keçdi və təxminən 1925-ci ildə bütün dünya üzrə kriminalda geniş tətbiq edilməyə başlandı.

Insan identifikasiyası üçün barmaq izinin tanınmasının geniş yayılmasına baxmayaraq, insanın barmağının papilyar cizgiləri şəklinin nadir xüsusiyyət olduğu hələ də elmi cəhətdən sübut edilməyib. Lakin bu texnologiyanın kriminal və digər sahələrdə istifadəsinə baxmayaraq, hələ də barmaq izi tamamil eyni olan iki insan tapılmayıb. XX əsrin ikinci yarısında yeni texnologiyaların yaranması ilə əlaqədar olaraq barmaq izinə görə tanınma sistemləri aşağıdakı sahələrdə tətbiq edilməyə başlandı:

1. Girişin idarəolunması sistemi.
2. Informasiya təhlükəsizliyi (şəbəkəyə giriş, FK-ə

giriş).

3. Iş saatının hesabatı və istifadəçilərin qeydiyyatı.

4. Səsvermə sistemləri.

5. Elektron ödənişin aparılması.

6. Insanların identifikasiyası tələb olunan müxtəlif sosial layihələr.

7. Vətəndaşın identifikasiyası layihələri (dövlət sərhəddinin keçilməsi, ölkəyə səfər üçün vizanın verilməsi və s.).

Gözün qüzehli qişası

İnsan gözünün qüzehli qişası barmaq izləri kimi onun unikal biometrik xarakteristikasıdır. Qüzehli qişanın şəklini analiz edən sistemlər kifayət qədər etibarlı tanımanı təmin edirlər. Bu xarakteristika yetərincə stabildir, insanın bütün həyatı boyunca praktik olaraq dəyişmir, çirklənməyə və yaralara qarşı həssas deyil. Qeyd edək ki, sağ və sol gözün qüzehli qişasının şəkli əhəmiyyətli dərəcədə fərqlənir.

Gözün qüzehli qişası üçün skanerlərin üstünlüyü ondan ibarətdir ki, onlar istifadəçidən diqqətini bir hədəfə cəmləşdirməsini tələb etmirlər, qüzehli qişada ləkə nümunələri gözün səthində yerləşir. Faktiki olaraq gözün videotəsvirini hətta bir metrdən az məsafədə çəkmək olar, bunun sayəsində də qüzehli qişa skanerləri bankomatlar üçün yararlı olur.

Gözün torlu qişası

Şəxsiyyətin ən etibarlı identifikasiya metodlarından biri gözün torlu qişasından istifadə edilməsidir. Göz dibini xarici işıq mənbəyi ilə işıqlandırdıqda gözün torlu qişası – gözü qanlatəchiz edən venalar və arteriyalar yaxşı görünür. Hələ 1935-ci ildə sübut olunmuşdu ki, hətta əkizlərdə belə

gözün torlu qişasının qan damarlarının şəkli üst-üstə düşmür. Gözün torlu qişası ilə tanınma metodu 1970-ci illərin ortalarından sənaye miqyasında inkişaf etməyə başladı.

Bu sistemlərdə skaner ya göz dibinin qan damarlarının şəklini, ya da torlu qişanın özünün əksetdirmə və udma xarakteristikalarını müəyyən edir. Xüsusi qurğuda qeyd olunmaq üçün gözcükdən məsafədəki işıqlı nöqtəyə bir dəqiqədən az müddətdə baxmaq lazımdır. Bu müddət ərzində sistem torlu qişanı işıqlandırır və əks olunmuş siqnalı alır. Torlu qişanı işıqlandırmaq üçün aşağı intensivlikli infraqırmızı şüalanma istifadə edilir, şüalar göz bəbəyindən keçərək gözün arxa divarındakı qan damarlarına yönəlir. Alınmış siqnaldan bir neçə yüz ilkin xarakterik nöqtə seçilir, onlar haqqında orta informasiya hesablanır və kodlanmış faylda saxlanır.

Bu metodun səhvləri yoxlanılan şəxsin başını etalondan kənara meyl etdirməsi və baxışlarını məsafədəki işıq mənbəyinə səhv fokuslaması ilə əlaqədardır. Sandiya milli laboratoriyasının (ABŞ) məlumatlarına görə bu metod üçün birinci növ səhvlər 0,4% təşkil edir. İkinci növ səhvlər praktiki olaraq mümkün deyil. Belə biometrik qurğuları aldada bilən mulyajın hazırlanmasının çətinliyi haqqında məlumatlar yoxdur. Həmçinin iddia edilir ki, təkrar edilməsi zəruri olan optik xassələr səbəbindən saxta torlu qişanın hazırlanması olduqca mürəkkəbdir. Gözün torlu qişası üçün skanerlər tam məxfi sistemlərə girişin təşkili zamanı geniş tətbiq edilir.

Sifət

Sifət cəmiyyətdə ən yaxşı qəbul edilən biometrik identifikatorlardan biridir, çünki vizual qarşılıqlı əlaqədə insanların geniş istifadə etdikləri tanıma üsuludur. Sifətin tanınması üçün bahalı xüsusi avadanlıq tələb olunmur. İdentifikasiya ilə yanaşı bir sıra digər funksiyalar da yerinə yetirən adi videomüşahidə kamerası da istifadə edilə bilər. İkincisi, qurğunun işə düşməsi üçün oxuma qurğusu ilə fiziki təmas, nəyəsə toxunmaq, müəyyən vəziyyəti almaq, hər hansı frazanı tələffüz etmək tələb olunmur. Tanıma prosesi təbii, bəzi hallarda identifikasiya edilənə hiss etdirilmədən baş verir.

Sifəti tanıma sistemlərinin əsasını xüsusi proqram təminatı təşkil edir, proqram sifət təsvirini adi veb-kamera ilə də götürür və onu emal edir. Sifətdə ayrı-ayrı obyektlər seçilir (qaşlar, gözlər, burun, dodaqlar), onların hər biri üçün onları tam müəyyən edən parametrlər hesablanır. Müasir sistemlərin çoxu bu zaman insan sifətinin üçölçülü obrazını yaradır. Bu ona görə lazımdır ki, məsələn, başı əydikdə və ya kiçik bucaq altında çevirdikdə identifikasiya mümkün olsun.

Hələlik sifəti tanıma texnologiyalarının inkişaf səviyyəsi kamillikdən uzaqdır – onlar 10 % səhv işə düşmə ilə təxminən 30 %-dən 70 %-ə qədər identifikasiya verir. Bu göstərici, məsələn, ABŞ aeroportlarından birində öz təsdiqini tapmışdı, 11 sentyabr 2001-ci il hadisələrindən sonra bu aeroportda sifəti tanıma sistemləri qurulmuşdu.

Əlin həndəsəsi

Sifətin həndəsi parametrlərini qiymətləndirən sistemlərlə yanaşı əlin həndəsi parametrlərini də ölçən qurğular var. Bu zaman 90-dan artıq müxtəlif

xarakteristika, o cümlədən, ovucun ölçüləri (üç ölçü), barmaqların uzunluğu və eni, oynaqların ümumi şəkli və s. ölçülür.

Əlin siluetinə görə identifikasiya sistemləri ilk biometrik qurğular kimi meydana çıxmışlar və onların seriya buraxılışına 1970-ci illərin əvvəlində başlanmışdı. Biometrik şablonun yığcamlığı baxımından bu növ sistemlər ən qənaətcil sistemlərdir. Barmaqların yalnız eni və uzunluğu haqqında informasiya saxlanıldıqda cəmisi 9 bayt tələb edilir. Təbii olaraq, yalnız barmaqların enini və uzunluğunu nəzərə alan sistemlər üçün həqiqi əlin karton mulyajını da asanlıqla hazırlamaq olar.

Əl imzası

Əl imzası da fizioloji xarakteristikalar kimi insanın unikal atributlarındandır. Bundan başqa bu istənilən insan üçün daha adi identifikasiya metodudur, çünki barmaq izinin götürülməsindən fərqli olaraq kriminalistika ilə assosiasiya yaratmır. Adətən imza haqqında verilənlərin iki emal üsulunu fərqləndirirlər: nümunə ilə sadə müqayisə və dinamik verifikasiya. Birinci olduqca etibarsızdır, çünki daxil edilən imzanın verilənlər bazasında saxlanan qrafiki nümunə ilə adi müqayisəsinə əsaslanır. Əl imzası həmişə eyni ola bilmədiyi üçün bu metod böyük səhv faizi verir. Dinamik verifikasiya üsulu xeyli mürəkkəb hesablamalar tələb edir və imza prosesinin imzanın müxtəlif sahələrində əlin hərəkət sürəti, təzyiq qüvvəsi, imzanın müxtəlif mərhələlərinin müddətləri kimi parametrlərini real vaxtda qeydə almağa kömək edir. Bu ona zəmanət verir ki, imzanı hətta təcrübəli qrafoloq da saxtalaşdıra bilməz, çünki heç kim imza sahibinin əlinin davranışını dəqiq yamsılamaq iqtidarında deyil.

İstifadəçi standart diqitayzer və qələmdən istifadə edərək öz adi imzasını təqlid edir, sistem isə hərəkətin parametrlərini oxuyur və onları əvvəlcədən verilənlər bazasına daxil edilmiş parametrlərlə müqayisə edir. İmza nümunəsi etalonla üst-üstə düşdükdə sistem imzalanan sənədə istifadəçinin adı, elektron-poçt ünvanı, vəzifəsi, cari zaman və tarix, imzanın parametrləri (hərəkət dinamikasının 10-dan çox xarakteristikası – istiqamət, sürət, təcil və s.) olan informasiyanı əlavə edir. Bu verilənlər şifrlənir, sonra onlar üçün nəzarət cəmi hesablanır, daha sonra bütün bunlar bir daha şifrlənir, beləliklə, biometrik şablon yaradılır. Sistemin sazlanması üçün yeni qeydə alınan istifadəçi 5-10 dəfə sənədin imzalanması prosedurunu yerinə yetirir, bu ortalanmış göstəricilər və etibarlıq intervalı almağa imkan verir. Bu texnologiyadan ilk dəfə PenOp şirkəti istifadə etmişdir.

Səs

Səs – sifət və ya barmaq izləri kimi hər bir insanın ayrılmaz əlamətidir. Rabitə vasitələrinin genişyayılması (stasionar və mobil telefon şəbəkələri, IP-telefoniya və s.) bu biometrik identifikatorun tətbiqi üçün böyük imkanlar açır; bundan başqa səs üzrə tanıma istifadəçilər üçün çox rahatdır və onlardan minimal səylər tələb edir.

İnsanın nitqi ayrıca «səs kadrlarına» bölünür, sonra onları rəqəmsal modelə çevirirlər. Bu modelləri «səs izləri» (voiceprint) adlandırırlar (barmaq izləri ilə analogiya).

Yaradılan «səs izi» bazada qeydə alınır. Səs üzrə identifikasiya kodunun qurulması üçün olduqca çox sayda üsul vardır, bir qayda olaraq onlar nitqin tezlik və statistik xarakteristikalarının müxtəlif cür əlaqələndirilməsidir. İdentifikasiya zamanı əvvəl qeydə alınmış və yeni

yaradılmış «səs izləri» müqayisə edilir. Etibarlığı artırmaq və tanımanı sürətləndirmək üçün çox vaxt istifadəçidən əvvəlcədən razılaşdırılmış suallara cavab verməsi və ya parolu tələffüz etməsi xahiş edilir.

Termoqramlar

Biometrik texnologiya kimi termoqramlar – insan bədəni hissələrinin infraqırmızı spektrin qısadalğalı (0,9-1,7 mkm), orta (3-5 mkm) və uzundalğalıd iapozonda alınmış təsvirləridir. Xüsusilə sifətin və əlin termoqramları sahəsində müxtəlif tədqiqatlar aparılmışdır. Adi təsvirlərlə müqayisədə termoqramların böyük üstünlüyü onların işıqlanmanın dəyişməsindən asılı olmamasıdır – sifət termoqramlarını tam qaranlıqda belə əldə etmək mümkündür.

Dodaqların hərəkəti

Danışıq zamanı dodaqların hərəkəti biometrik davranış parametrlərinə aiddir. Ondan səsin tanınması sisteminə vizual əlavə kimi istifadə etmək olar. Dodaqların hərəkətinə görə autentifikasiya texnologiyasının növləri danışanın tanınması sistemindəki kimidir: sabit mətn, mətndən asılı və mətndən asılı olmayan. Son dövrlər M2VTS verilənlər bazasının yayılması sayəsində bu sahədə tədqiqatlar çoxalmağa başlamışdır.

Bazarda BioID firmasının dodaqların hərəkətinə əsaslanan biometrik sistemi meydana çıxmışdır. Bu metodun ən böyük üstünlüklərindən biri onu asanlıqla səsin identifikasiyası və sifət üzrə identifikasiya ilə birləşdirmək imkanıdır. Bu yolla aldadılması mürəkkəb olan çox dəqiq sistemlər yaratmaq olar. Belə üçqat biometrik sistem fiziki girişə nəzarət üçündür, kamera qarşısında mikrofona danışan insanın parametrləri oxunur. Videotəsvir sifət

həndəsəsinin analizi üçün istifadə edilir və dodaqlarının hərəkətinin, onların nəticələri səs üzrə identifikasiyanın nəticələri ilə birləşdirilir.

Klaviatura xətti

Klaviatura xətti ilə identifikasiya insanın məxsusi çap üslubu ilə identifikasiyasıdır.

Hər bir insanın xarakterik çap xüsusiyyətləri var: klavişlərin basılmaları arasındakı zaman intervalları və klavişlərin basılı vəziyyətdə saxlanması zamanları hər bir insan üçün müəyyən qədər sabitdir. Klaviatura xətti ilə identifikasiya sistemləri sabit parola əsaslanırlar, lakin səsin tanınmasında olduğu kimi mətndən asılı olmaya da bilərlər. Mətnin yığılması zamanının hesablanması əsasında klaviatura xəttinə görə tanıma üçün kommersiya məhsulları mövcuddur.

§9. Virtual xüsusi şəbəkələr (VPN). VPN təsnifatı

Şəbəkə hücumlarının qarşısının effektiv alınması, açıq şəbəkələrin gündəlik fəaliyyətdə fəal və təhlükəsiz istifadəsi imkanlarının təmin edilməsi üçün qorunan virtual xüsusi şəbəkələrin (VPN – Virtual Private Networks) qurulması konsepsiyasından, eləcə də onların reallaşdırılması və tətbiqi texnologiyasından istifadə olunur.

Qorunan virtual xüsusi şəbəkələrin (VPN) qurulması konsepsiyasının əsasında aşağıdakı kimi çox sadə ideya

durur. Əgər qlobal şəbəkənin iki qovşağı öz aralarında məlumat mübadiləsi aparmaq istəyirsə, onda onlar arasında açıq şəbəkə vasitəsilə ötürülən informasiyanın məxfiliyini və tamlığını təmin etmək üçün bütün mümkün aktiv və passiv xarici müşahidəçilərin girişinin əlahiddə çətinləşdirildiyi virtual tunelin qurulması zəruridir. Burada "virtual" sözü iki qovşaq arasında birləşmənin daimi olmadığını və yalnız trafikin şəbəkədən keçdiyi zaman mövcud olduğunu göstərmək məqsədilə istifadə edilir.

VPN dedikdə açıq xarici informasiya ötürmə mühiti vasitəsilə dövr edən məlumatlarının təhlükəsizliyini təmin etmək üçün lokal şəbəkələrin və ayrı-ayrı kompüterlərin vahid virtual korporativ şəbəkədə birləşdirilməsi başa düşülür.

Qeyd etmək lazımdır ki, korporativ (o cümlədən lokal) şəbəkələrin açıq kompüter şəbəkəsinə, o cümlədən İnternetə qoşulması zamanı iki növ təhlükə meydana çıxır:

- korporativ istifadə olunan məlumatlara açıq şəbəkə ilə ötürülmə prosesində icazəsiz girişin əldə olunması;
- bədniyyətli şəxs tərəfindən korporativ (o cümlədən lokal) şəbəkəyə icazəsiz daxilolma nəticəsində bu şəbəkəni daxili resurslarına icazəsiz girişin əldə edilməsi.

Ona görə də açıq rabitə kanalları ilə ötürülərkən informasiyanın qorunması kriptoqrafik üsulların əsasında reallaşdırılan aşağıdakı əsas funksiyaların bir-biri ilə qarşılıqlı əlaqə şəkildə yerinə yetirilməsinə əsaslanır:

- qarşılıqlı əlaqədə olan tərəflərin autentifikasiyası;
- ötürülən məlumatların kriptoqrafik şifrlənməsi;
- ünvana çatdırılan məlumatlarının həqiqiliyinin və tamlığının yoxlanılması.

Açıq rabitə kanalları ilə ötürülməsi zamanı

informasiyanın qorunması kriptoqrafik qorunan tunellər adlanan qorunan virtual rabitə kanallarının qurulması prinsipinə əsaslanır.

Kriptoqrafik qorunan tunel özündə kriptoqrafik qorunan məlumat paketlərinin ötürülməsi üçün istifadə olunan və açıq kompüter şəbəkəsindən keçən birləşməni ehtiva edir.

İki qovşaq arasında qorunan tunelin yaradılması virtual şəbəkənin həmin qovşaqlarda fəaliyyət göstərən, tunelin təşəbbüskarı və terminatoru adlanan komponentləri tərəfindən həyata keçirilir. Burada təşəbbüskar – tuneli yaradan və paketləri göndərən tərəf, terminator isə tunel vasitəsilə paketləri alan tərəfdir.

Tunelin təşəbbüskarı göndərilən paketi yeni paketin içərisinə qoyur. Yeni paket ilkin məlumatlarla yanaşı göndərən və alan haqqında informasiyaya malik olan yeni başlığı özündə saxlayır.

Tunel vasitəsilə ötürülən bütün paketlərin IP paket olmasına baxmayaraq, onun içərisinə yerləşdirilən paketlər istənilən növ protokola, hətta NetBEUI tipli marşrutlaşdırılmayan protokollara da aid ola bilər. Tunelin təşəbbüskarı ilə terminatoru arasındakı marşrut adi marşrutlaşdırılan IP şəbəkədir. Bu şəbəkə qismində İnternetdən fərqli istənilən şəbəkə çıxış edə bilər.

Tunelin terminatoru əks əməliyyatı yerinə yetirir, yəni o, aldığı paketdən əlavə olunmuş başlığı silir, qalan ilkin paketi lokal şəbəkədə ünvana göndərir və ya lokal paketlər stekinə yerləşdirir.

Göndərilən paketin yeni paketin içərisinə yerləşdirilməsi özlüyündə tunel vasitəsilə ötürülən məlumat paketlərinin qorunmasına təsir etmir. Lakin bu, yeni paketin içərisinə yerləşdirilən ilkin paketin tam krip-

toqrafik qorunmasına imkan verir. Belə ki, ilkin paketin məxfiliyi onun kriptoqrafik şifrlənməsi, tamlığı isə rəqəm imzanın reallaşdırılması yolu ilə təmin edilir. Bu zaman tunelin təşəbbüskarı və terminatoru açarların təhlükəsiz mübadiləsi üçün müvafiq mexanizmlərdən istifadə etməlidirlər.

Tunelin yalnız səlahiyyət verilmiş iki istifadəçi arasında yaradılması həmin tərəflərin qarşılıqlı autentifikasiyasının aparılması yolu ilə təmin edilir.

Virtual xüsusi şəbəkələrin təsnifatı

VPN şəbəkələrı əsasən üç əlamətə görə təsnif edirlər:

- açıq sistemlərın qarşılıqlı əlaqə (OSI) modelinin səviyyələri üzrə təsnifat;
- texniki həllin arxitekturasına görə təsnifat;
- texniki reallaşdırma usullarına görə təsnifat.

VPN şəbəkəsinin OSI modelinin səviyyələri üzrə təsnifatı

Ümumi girişli (qorunmayan) şəbəkə ilə məlumatların təhlükəsiz ötürülməsi texnologiyası üçün ümumiləşdirilmiş anlayış olan qorunan kanal tətbiq edilir. Qorunan kanalı OSI modelinin müxtəlif səviyyələrində reallaşdırılan sistem vasitələrinin köməyi ilə qurmaq olar.

Reallaşdırılan VPN şəbəkələrin funksionallığı OSI modelinin seçilmiş səviyyəsindən, onun sistem əlavələri və digər qoruma vasitələri ilə uzlaşmasından çox asılıdır. VPN şəbəkəsinin reallaşdırılması üçün seçilən OSI modelinin səviyyələrinə görə onlartı üç qrupa bölürlər:

- kanal səviyyəsinin VPN şəbəkəsi;
- şəbəkə səviyyəsinin VPN şəbəkəsi;
- seans səviyyəsinin VPN şəbəkəsi.

VPN şəbəkələr OSI modelinin ən aşağı səviyyələrində qurulur. Belə ki, kanalın qorunması vasitələri nə qədər

aşağı səviyyədə reallaşdırılarsa, bu vasitələri proqram əlavələri və tətbiqi protokollar üçün şəffaf etmək bir o qədər asan olur. Lakin burada qoruma protokolunun konkret şəbəkə texnologiyasından asılılığı problemi yaranır.

Qoruma vasitələrinin OSI modelinin yuxarı (tətbiqi və ya təqdimat) səviyyələrdə reallaşdırılmasının üstün cəhəti ondan ibarətdir ki, bu zaman həmin vasitələr şəbəkə platformasından asılı olmur. Lakin bu halda reallaşdırılan proqram əlavələrinin konkret qoruma protokolundan asılılığını, başqa sözlə, qoruma protokollarının belə proqram əlavələri üçün şəffaf olmamasını çatışmazlıq qismində göstərmək olar.

Ən yüksək (tətbiqi) səviyyədə reallaşdırılan qorunan kanalın daha bir çatışmazlığı fəaliyyət sahəsinin məhdud olması ilə bağlıdır. Bu halda protokol yalnız bir şəbəkə xidmətini (məsələn, FTP, HTTP, SMTP) qorumağa imkan verir. Ona görə də hər bir xidmət üçün protokolun müvafiq qorunan versiyasını işləyib hazırlamaq tələb olunur. Məsələn, S/MIME protokolu yalnız elektron poçtunu qorumaq üçün reallaşdırılmışdır. Nəzərə alınmalıdır ki, OSI modelinin yuxarı səviyyələrində protokolların istifadə olunan steki ilə proqram əlavəsi arasında ciddi əlaqə mövcud olur.

OSI modelinin kanal səviyyəsinin VPN şəbəkəsi.

OSI modelinin kanal səviyyəsində istifadə olunan VPN vasitələr üçüncü və daha yuxarı səviyyələrin trafikinin müxtəlif növlərini qorumağa və "nöqtə-nöqtə" formatlı virtual tunellər qurmağa imkan verir. Bu qrup VPN şəbəkələrə Cisco Systems və Microsoft şirkətləri tərəfindən işlənib hazırlanmış L2F (Layer 2 Forwarding),

PPTP (Point-to-Point Tunelling Protocol) və L2TP (Layer 2 Tunelling Protocol) protokollarını istifadə edən vasitələr aid edilir.

Qorunan kanalın PPTP protokolu PPP protokoluna əsaslanır və qoruma vasitələrinin tətbiqi səviyyənin proqram əlavələri və xidmətləri üçün şəffaflığını təmin edir. Bu protokol IP şəbəkələri ilə yanaşı, IPX, DECnet və ya NetBEUI protokolları ilə işləyən şəbəkələrdə də paketləri təhlükəsiz ötürməyə imkan verir.

L2TP protokolu lokal şəbəkələrdə uzaq məsafədən girişin təşkili zamanı istifadə olunur.

OSI modelinin şəbəkə səviyyəsinin VPN şəbəkəsi.

Şəbəkə səviyyəsinin VPN vasitələri IP paketlərin IP paketlərə qoyulmasını yerinə yetirir. Bu səviyyədə reallaşdırılan məlum protokollardan biri SKIP protokoludur. Tədricən bu protokolu IP paketlərin autentifikasiyası, tunelləşdirilməsi və şifrlənməsi üçün nəzərdə tutulan və şəbəkə səviyyəsində işləyən IPSec protokolu əvəz edir. Bu protokol kompromis variant təqdim edir. Belə ki, o, bir tərəfdən proqram əlavələri üçün şəffafdır, digər tərəfdən isə IP protokoluna əsaslandığı üçün bütün şəbəkələrdə işləyə bilər.

Tunel qurularkən IPSec protokolu istifadəçilərin və ya kompüterlərin identifikasiyası, tunelin son nöqtələrində şifrləmənin istifadəsi, eləcə də şifrləmə açarlarının mübadiləsi və idarə edilməsi üçün standart üsullar nəzərdə tutur. IPSec protokolu L2TP protokolu ilə birgə işləyə bilir ki, bu da daha etibarlı identifikasiyanı, standartlaşdırılmış şifrləməni və məlumatların tamlığını təmin edir. IPSec tuneli iki lokal şəbəkə arasında məlumatın ötürülməsi üçün çoxlu sayda fərdi kanalları reallaşdırmağa

imkan verir. Ona görə də IPSec protokolu miqyas baxımından üstünlüklərə malikdir.

Qeyd olunmalıdır ki, ötürülən informasiyanı kənar müdaxilədən qorumağa, uzaq məsafədə olan qurğular arasında kriptoqrafik açarları təhlükəsiz mübadilə və idarə etməyə imkan verən IKE protokolundan da istifadə olunur.

OSI modelinin seans səviyyəsinin VPN şəbəkəsi.

Bəzi VPN şəbəkələr "kanal vasitəçiləri" üsulundan isti fadə edirlər. Onlar nəqliyyat səviyyəsinin üzərində qurulur və trafiki qorunan şəbəkədən İnternetə ötürür. Belə tunelin təşəbbüskarı və terminatoru arasında ötürülən informasiyanın şifrlənməsi çox vaxt nəqliyyat səviyyəsinin qorunması (TSL) vasitəsilə həyata keçirilir.

ŞE-dən keçidin autentifikasiyasını standartlaşdırmaq məqsədilə IETF konsorsiumu tərəfindən SOCKS protokolu təklif edilmişdir. Hazırda SOCKS v.5 protokolu kanal vasitəçilərinin standart reallaşdırılması üçün tətbiq olunur. Potokola əsasən vasitəçi rolunu oynayan kompüterlə server arasında autentifikasiya olunmuş soket və ya seans qurulur. Bu halda həmin vasitəçi ŞE vasitəsilə əlaqə üçün yeganə yol rolunu oynayır və müştəri (kliyent) tərəfindən sifariş olunan istənilən əməliyyatı yerinə yetirir. Vasitəçinin soket səviyyəsində trafik haqqında məlumatı olduğuna görə o, ciddi nəzarət həyata keçirə (əgər istifadəçi zəruru səahiyyətlərə malik deyilsə, onda onların konkret proqram əlavələrini dayandıra) bilər.

Texniki həllin arxitekturasına görə VPN şəbəkələrin təsnifatı

Texniki həllin arxitekturasına görə VPN şəbəkələr üç növə ayrılır:

- uzaq məsafədən girişli VPN (Remote Access VPN);

- korporativ şəbəkə daxili VPN (intranet VPN);
- korporativ şəbəkələr arası VPN (extranet VPN).

Uzaq məsafədən girişli VPN şəbəkələr. Remote Access VPN şəbəkələr təşkilatın mobil fəaliyyətdə və uzaqdan olan əməkdaşının korporativ informasiya resursla- rına uzaq məsafədən təhlükəsiz girişi təmin etmək üçün nəzərdə tutulmuşdur.

Korporativ şəbəkə daxili VPN şəbəkələr. İntranet VPN şəbəkələr kompüter şəbəkələri vasitəsilə birləşdirilmiş təşkilat daxili struktur bölmələr və ya təşkilatlar qrupu arasında qorunan qarşılıqlı fəaliyyəti təmin edir.

Korporativ şəbəkələr arası VPN şəbəkələr. Extranet VPN təşkilatın əməkdaşlarına strateji tərəfdaşları, tədarükçü, böyük sifarişçi, istifadəçi, müştəri və s. ilə qorunan informasiya mübadiləsini təmin edir. Bu şəbəkələr bir təşkilatın kompüter şəbəkəsindən digər təşkilatın kompüter şəbəkəsinə birbaşa girişi təmin edir və bu zaman işgüzar əməkdaşlığın gedişində rabitənin etibarlığını yüksəltməyə imkan verir. Extranet VPN şəbəkələrdə əsas diqqət ŞE vasitəsilə girişə nəzarət və istifadəçilərin autentifikasiyası məsələlərinə yönəlir.

Texniki reallaşdırma üsullarına görə VPN şəbəkələrin təsnifatı

Texniki reallaşdırma üsullarına görə VPN şəbəkələr beş qrupa bölünür:

- şəbəkə əməliyyat sistemi əsasında VPN;
- ŞE əsasında VPN;
- marşrutlayıcılar əsasında VPN;
- proqram təminatı əsasında VPN;
- daxili şifrprosessoru olan xüsusiləşdirilmiş apparat vasitələri əsasında VPN.

Şəbəkə əməliyyat sistemi əsasında VPN. Bu növ VPN şəbəkəni yaratmaq üçün Microsoft şirkəti Windows NT şəbəkə əməliyyat sisteminə inteqrasiya edilmiş PPTP protokolunu təklif edir. Korporativ əməliyyat sistemi qismində Windows NT sistemini istifadə eən təşkilatlar üçün belə həll cəlbedici görünür. Windows NT bazasında qurulan VPN şəbəkələrdə PDC (Primary Domain Controller) kontrollerdə saxlanılan kliyent məlumat bazaları istifadə olunur.

İstifadəçi PPTP serverə qoşulan zaman PAP, CHAP və ya MS CHAP protokolları üzrə yoxlanılır. Məlumatların şifrlənməsi üçün 40 bitlik açarla işləyən qeyri-standart Point-to-Point Encryption protokolu tətbiq olunur. Belə yanaşmanın üstünlüyü kimi onun əhəmiyyətli dərəcədə ucuz olmasını, çatışmazlığı qismində isə PPTP protokolunun qorunmasının kifayət qədər yüksək olmamasını göstərmək olar.

ŞE əsasında VPN. Əksər istehsalçıların ŞE-ləri məlumatların tunelləşdirilməsi və şifrlənməsi funksiyalarını reallaşdırır. Bir qayda olaraq, ŞE-nin proqram təminatının tərkibinə şifrləmə modulu əlavə edilir. Bu üsulun çatışmazlığı qismində həllin yüksək qiymətə malik olması göstərilir. ŞE-nin fərdi kompüterlərin bazasında istifadəsi zamanı nəzərə almaq lazımdır ki, belə yanaş manın yalnız məhdud həcmli məlumatların ötürüldüyü kiçik şəbəkələr üçün reallaşdırılması məqsədəmüvafiqdir.

Marşrutlayıcılar əsasında VPN. Belə VPN şəbəkəsinin qurulması üsulu qorunan kanalların yaradılması üçün marşrutlayıcıların tətbiqini nəzərdə tutur. Belə ki, lokal şəbəkədən çıxan bütün məlumatların marşrutlayıcıdan

keçdiyini nəzərə alaraq, şifrləmə məsələsinin də onun üzərinə qoyulması daha əlverişli hesab edilir.

Proqram təminatı əsasında VPN. Belə VPN şəbəkələrin qurulması üçün ayrıca kompüterdə işləyən və əksər hallarda proxy-server funksiyalarını yerinə yetirən xüsusi proqram təminatından istifadə olunur. Belə proqram təminatına malik olan kompüter şəbəkədə ŞE-dən sonra yerləşdirilə bilər.

Daxili şifrprosessoru olan xüsusi aparat vasitələri əsasında VPN. Belə VPN şəbəkələr yüksək səmərəlilik və məhsuldarlıq tələb olunan şəbəkələrdə tətbiq edilə bilər. Çatışmazlığı - qiymətin yüksək olmasıdır.

§10. Kriptoqrafiyanın əsas anlayışları və məqsədləri. Kriptoqrafiyanın şifrələnmə üsulları.

Kriptologiya – qədim elmdir və adətən Yuliy Sezar haqqında söhbət getdikdə, bu haqda danışıq (bizim eradan 100-44 il əvvəl) gedir. Qədim romada Sezarın Çiçeron və digər "abonentlərlə" məktub yazışmasında (bizim eradan 106-43-cü illər) şifrləmə üsulundan istifadə edilmişdir.Sezarın şifrində, başqa sözlə desək dövri yerdəyişmələrdə məlumatda hər bir hərf əlifbada ondan müəyyən hərflər miqdarı qədər geridə olan hərflə əvəz olunur. Sezar hər bir hərfi, həmin hərfdən 3 hərf arxada olan hərflə əvəz etmişdir. Bu günkü gündə simvollarla əməliyyatı yerinə yetirdikdə, əməliyyatda hərflər yox,

həmin hərflərə uyğun olan ədədlər iştirak edirlər.

Latın əlifbasında A-ya uyğun olan "0"-dan Z-ə uyğun olan 26-ə qədər ədədlərdən istifadə etmək olar. İlkin simvola uyğun gələn ədədi X ilə, kodlaşdırılmış ədədi isə Y ilə işarə etsək, o zaman əvəzedici şifrin tətbiq olunma qaydası belə olacaq: $Y=x+z(\text{mod } N)$, (1). Burada z-məxfi açar, N - əlifbadakı smvolların miqdarı, N moduluna görə toplama isə - adi toplamaya oxşar bir əməl olub, adi toplamadan fərq ondan ibarətdir ki, əgər adi toplamada nəticə N- dən böyük və ya ona bərabər olduğu halda, ikinci halda cəmin qiyməti onun N-ə böldükdə alınmış qalığa bərabər qəbul edilir.

Kriptologiya – şifrləmə üsullarını öyrənən və ya məlumatın doğruluğunu yoxlayan kriptoqrafiya və aydınlaşdırma olumu tədqiq edən və kriptoqramı əvəz edən kriptonaliz kimi 2 hissədən ibarətdir. Kriptoqrafiyada ilk sistematik əsər kimi böyük arxitektor Leon Battista Albertininin əsərini göstərmək olar. XVII əsrin ortalarına qədər kriptoqrafiya və kriptoanaliz üzrə külli miqdarda işlər meydana gəlmişdir. O vaxtlar şifroqram üzrə Avropada çox maraqlı hadisələr baş vermişdir.

Kriptologiya sahəsində növbəti məşhur şəxs – hollandiyalı Oqyust Kerkhoff (1835-1903-cü illər) olmuşdur. Çox qiymətli olan "Kerkhoff qaydası" ona məxsusdur. Bu qaydaya görə "şifrin davamlılığı yalnız açarın məxfiliyi ilə təyin olunur". AT&T-in mühəndisi Jilber Vernamdır. 1926-cı ildə o, həqiqətən dəaçılmayan şifr təklif etmişdi. Şifrin ideyası ondan ibarət idi ki, (1) tənliyində hər bir növbəti simvol üçün Z-in yeni qiymətini seçmək lazımdır. Məxfi açardan yalnız bir dəfə istifadə olunmalıdır. Əgər bu açar təsadüf nəticəsində seçilirsə,

Şennon tərəfindən 23 il əvvəl ciddi sübut olunmuş nəzəriyyəyə görə belə şifr açılmazdır.

II dünya müharibəsində geniş tətbiq olunmağa başlanmış "şifr-bloknot"-lardan istifadə olunmasının nəzəri əsaslarını məhz həmin açılmaz şifr təşkil edir. Şifrləməmişdən əvvəl, informasiyanı statik kodlaşdırmaq lazımdır (sıxlaşdırmaq, arxivləşdirmək). Bu halda informasiyanın həcmi və izafiliyi azalacaq, entropiya yüksələcəkdir (bir simvola uyğun olan informasiyanın orta miqdarı).

"Kriptoqrafiya" sözü yunan dilində "kryptos" – məxfi və "grapho" – yazı sözlərindən yaranmışdır. Bu terminin mənası kriptoqrafiyanın əsas təyinatını ifadə edir – vacib məlumatı mühafizə etmək və ya məxfi saxlamaq.

Kriptoqrafik şifrələnmə üsulları.

Haker hücumlarının əsas məqsədi təkcə kompüterdə olan informasiyanın məhv edilməsi deyil, həm də onların icazəsiz ―ələ keçirilməsidir. Əgər bunun qarşısını texniki vasitələrin köməyilə almaq mümkün olmursa, onda şifrləmə sistemindən istifadə olunur. Şifrləmə üsulları ilə kriptoqrafiya məşğul olur. Müasir kriptoqrafiyanın predmeti informasiyanı bədniyyətlinin müəyyən əməllərindən mühafizə etmək üçün istifadə edilən informasiya çevirmələridir.

Kriptoqrafiya konfidensiallığı, bütövlüyə nəzarəti, autentikasiyanı və müəlliflikdən imtinanın qeyri-mümkünlüyünü təmin etmək üçün tətbiq edilir. «Kriptoqrafiya» sözü kryptos ('gizli') və graphos ('yazı') yunan sözlərindən yaranmışdır. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur. Kriptoqrafik alqoritm – məlumatların

çevrilməsinin müəyyən üsuludur. Açar isə çevirmə üsulunu konkretləşdirir. Müasir kriptoqrafiya o prinsipdən çıxış edir ki, kriptoqrafik çevirmənin məxfiliyi yalnız açarın məxfi saxlanması ilə təmin edilməlidir.

İnformasiyanın kriptoqrafik müdafiəsinin prinsipləri

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var. Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları var. Simmetrik şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish kimi blok şifrləri və bir sıra axın şifrləri (RC4, A5) daha geniş istifadə olunur. Simmetrik şifrləmənin əsas nöqsanı ondan ibarətdir ki, məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Bu bir tərəfdən məxfi açarların tam məxfi kanalla göndərilməsi problemini yaradır. Digər tərəfdən alan tərəf şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən almasını sübut edə bilməz. Çünki belə məlumatı o özü də yarada bilər.

Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir.

Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA,

ElGamal, Şnorr və s. alqoritmlərini göstərmək olar.

Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla simmetrik metodla şifrlənir, sonra həmin təsadüfi açarı alan tərəfin açıq asimmetrik açarı ilə şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə, (istifadəçi, açıq açar) cütünün həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün rəqəmsal sertifikatdan istifadə edilir. Rəqəmsal sertifikat xüsusi sertifikasiya mərkəzləri tərəfindən verilir.

Rəqəmsal sertifikatda aşağıdakı verilənlər olur:

- sertifikatın seriya nömrəsi;
- sertifikatın sahibinin adı;
- sertifikatın sahibinin açıq açarı;
- sertifikatın fəaliyyət müddəti;
- elektron imza alqoritminin identifikatoru;
- sertifikasiya mərkəzinin adı və s.

Sertifikat onu verən sertifikasiya mərkəzinin rəqəmsal imzası ilə təsdiq edilir.

Heş-funksiyalar

Bütövlüyə nəzarət üçün kriptoqrafik heş-funksiyalar istifadə edilir. Heş-funksiya adətən müəyyən alqoritm şəklində realizə edilir, belə alqoritm ixtiyari uzunluqlu məlumat üçün uzunluğu sabit heş-kod hesablamağa imkan verir. Praktikada 128 bit və daha artıq uzunluqda heş-kod generasiya edən heş-funksiyalardan istifadə edilir.

Heş-funksiyanın xassələri elədir ki, onun köməyi ilə

alınan heş-kod məlumatla ―möhkəm‖ bağlı olur. Məlumatın hətta bir biti dəyişdikdə belə heş-kodun bitlərinin yarısı dəyişir. Heş-funksiyaya misal olaraq MD2, MD4, MD5, RIPEMD, SHA1 və s. alqoritmlərini göstərmək olar.

Misal. ‗1234567890‘ sətri üçün SHA1 heş-funksiya alqoritminin hesabladığı heşkod 16-lıq say sistemində 01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A simvollar ardıcıllığıdır. İnformasiya gizlədilməsinin kriptoqrafik üsullarının təsnifatı aşağıdakı şəkildə verilmişdir: Heş-funksiyadan istifadə Kompüter sisteminin istifadəçilərinin parollarını şifrləmək və elektron imza yaratmaqdan ötrü xeşləmə funksiyasından geniş istifadə olunur. Onlar istənilən uzunluqlu məlumatı qeyd edilmiş ölçülü sətirdə təsvir edirlər.

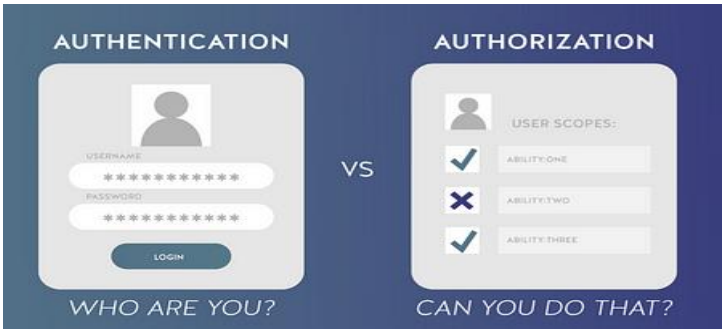
Onun tətbiqinin xüsusiyyəti ondan ibarət olur ki, sıxlaşdırılmış təsvirə görə ilkin məlumatın bərpa edilməsi mümkün olmur – buna bir tərəfli xeş-funksiya deyilir. İstifadəçilərin parollarının olduqları və xeş-funksiya vasitəsilə çevrilmiş faylı öz əlinə keçirən cinayətkar onun əsasında parolları əldə etmək imkanına malik olmur; bu məqsədlə o, simvolların parol kombinasiyalarını bir-bir seçməli, onlara xeş-funksiya tətbiq etməli və alınmış sətirlərin və xeşləndirilmiş parollar faylının sətri ilə uyğunluğunu yoxlamalıdır. Bu iş onunla çətinləşir ki, parolunun uzunluğu da məlum olmur.

§11. Parolun identifikasiya, autentifikasiya və avtorizasiyası. Birdəfəlik parollar.

Autentifikasiya və inzibatçıların sistemləri və məlumatları qorumaq üçün istifadə etdiyi iki mühüm informasiya təhlükəsizliyi prosesidir.

Autentifikasiya — istifadəçinin və ya xidmətin şəxsiyyətini yoxlayır.

Avtorizasiya — burada giriş hüquqlarını müəyyən edir.



Şəkildən də göründüyü kimi burada:

Autentifikasiya yəni (Doğrulama) Sən kimsən? sualına, Avtorizasiya isə Sən bunu edə bilərsən? sualına cavab verir.

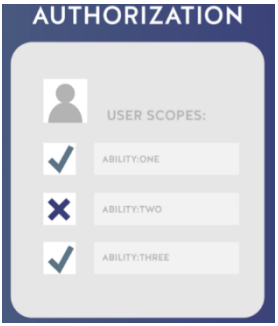
Autentifikasiya fərdi istifadəçinin ətraf mühitə daxil olmaq hüququnun təsdiqlənməsi və ya rədd edilməsidir. Yəni ki,resurslara girişə icazə verməzdən əvvəl istifadəçinin həqiqətən kim olduğunu sübut etmək üçün bir proses kimi işləyir. Proses aşağıdakı addımlarla işləyir:

Daxil olmağa cəhd edən istifadəçinin düzgün məlumatlara malik olduğunu təsdiqləmək (məs: istifadəçi adı, parol, biometrik məlumatlar, cihaz məlumatları)

Müəyyən edilmiş giriş nəzarətlərinin istifadəçiyə xüsusi

mühitə daxil olmasına icazə verdiyini təsdiqləmək.

Avtorizasiya şəxsiyyəti təmin etmək üçün növbəti addımdır. İstifadəçinin autentifikasiya yolu ilə mühitə daxil olması təsdiqləndikdən sonra avtorizasiya baş verir. Lakin sonra isə giriş nəzarətləri və qrup parametrləri vasitəsilə avtorizasiya istifadəçiyə daxil olmağa icazə verilən unikal resursları və məhdudlaşdırılan resursları müəyyən edir.



Həmçinin sadə desək belə də deyə bilərik. **Autentifikasiya** — istifadəçinin daxil etdiyi parolu verilənlər bazasında saxlanılan parolla müqayisə etməklə istifadəçinin şəxsiyyətini yoxlamaq prosedurudur. **Avtorizasiya** — müəyyən bir şəxsə müəyyən hərəkətlər etmək hüququ verilməsidir. **İdentifikasiya** — bir prosedurdur ki, bunun nəticəsində subyekt üçün onun unikal xüsusiyyəti aşkar edilir və onu informasiya sistemində unikal şəkildə müəyyən edir.

Praktiki nümunə ilə bu 3 əsas identifikasiya, avtorizasiya və autentifikasiyanı birlikdə tam başa düşək.

Məsələn: İstifadəçi öz Google hesabına daxil olmaq istəyir. Bu zaman sistem login tələb edir, istifadəçi onu yazır, sistem onu mövcud kimi tanıyır — bu

identifikasiyadır. Bundan sonra Google şifrə daxil etməyi tələb edir, istifadəçi onu daxil edir və sistem istifadəçinin həqiqətən real olduğuna razılaşır, çünki şifrə uyğun gəlir — bu autentifikasiyadır.

Ola bilər ki, Google əlavə olaraq SMS və ya proqramdan birdəfəlik kod istəyəcək. İstifadəçi onu düzgün daxil edərsə, sistem sonunda hesabın həqiqi sahibi olduğuna razı olacaq — bu iki faktorlu autentifikasiyadır. Sonra isə sistem istifadəçiyə poçt qutusundakı məktubları oxumaq və qalan əməliyyatları yerinə yetirmək hüququ verəcək bu isə artıq avtorizasiyadır.

TOTP — vaxt əsaslı birdəfəlik parollar alqoritmi

Adi istifadəçi adı və parola əsaslanan kimliyin təsdiqləmə (authentication) sistemlərinin zəif tərəfləri haqqında uzun danışmaq olar, amma bütün oxucular razılaşar ki, bu cür sistemlərin təhlükəsizliyi ilk növbədə istifadəçinin bilik səviyyəsindən, vərdişlərindən və nizam-intizamından asılıdır. Parolun statik olması onun cinayətkarların əlinə keçən zaman təkrar istifadəsinə imkan yaradır. Bu problemi aradan qaldırmaq üçün çoxfaktorlu təsdiqləmə sistemlərindən istifadə etmək olar. Çoxfaktorlu təsdiqləmə ilə müdafiə olunan istifadəçilər phishing, bruteforce, keylogger və digər oxşar risklərdən qurtulmuş olurlar. Bu cür sistemlərin sayı çoxdur (U2F, Fido2, mOTP), lakin həm istifadəsi, həm tətbiq edilməsi baxımından ən rahat və sadəsi TOTP alqoritmi əsasında olanlardı.

TOTP əsaslı çoxfaktorlu təsdiqləmə sistemlərinin iş prinsipini ən sadə izahatı belədir: adi istifadəçi adı və parol daxil etdikdən sonra, istifadəçi ikinci mərhələdə xüsusi

qurğu və ya mobil tətbiq tərəfindən yaradılan birdəfəlik parolu daxil etməlidir. Bu, adətən 6 və ya 8 rəqəmdən ibarət, parol server tərəfindən yoxlandıqdan sonra istifadəçiyə sistemə giriş icazəsi verilir.

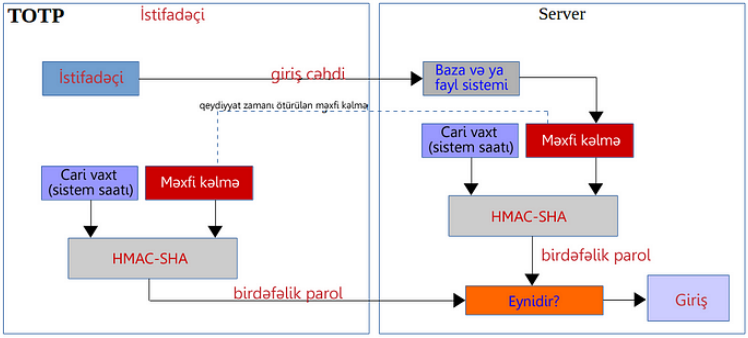
Birdəfəlik parollar xüsusi həş (hash) alqoritmi vasitəsi ilə hesablanır.

OTP = TOTP (time+shared secret)

Bu alqoritm HMAC və SHA-1/SHA-2 birləşməsindən ibarətdir və funksiya arqumenti iki hissədən ibarətdir :

1) time — cari vaxt (unix timestamp formatında)

2) shared secret- xüsusi məxfi kəlmə (həm server həm istifadəçiyə "məlum" bir parametr)



TOTP əsasında giriş alqoritminin sxeması

İstifadəçi qeydiyyatı zamanı xüsusi məxfi kəlmə server tərəfində təsadüfi şəkildə yaradılıb istifadəçiyə ötürülür (bir çox hallarda QR kod formatında). İstifadəçi həmin kəlməni TOTP protokolunu dəstəkləyən mobil tətbiqə daxil edir (və ya kamera vasitəsi ilə QR kodu oxuyur) və bununla qeydiyyat əməliyyatını başa çatdırır. Bu kod yalnız bir dəfə göstərilir və sonrakı əməliyyatlarda (yəni sistemə giriş zamanı) heç bir istiqamətdə ötürülmür.

TOTP profilinin qeydiyyatı üçün QR kod nümunəsi

TOTP funksiyası vaxt əsasında olduğuna görə, onun icrası nəticəsində yaranan birdəfəlik parollar hər saniyə dəyişir və unikal olur. Rahatlıq üçün, vaxt kəmiyyətini adətən 30 və ya 60 saniyəyədək yuvarladırlar.

Bir çox sistemlərin girişi üçün ikinci faktoru olaraq məhz TOTP istifadə olunur. Numunə kimi Facebook, Google, Office365 və Dropbox-un adını çəkmək olar.

TOTP olduqca sadə bir sistemdir və kifayət qədər məşhur olduğu üçün əksər proqramlaşdırma dilləri üçün hazır kitabxanaları və kod nümunələri var. Bundan əlavə bir çox sistemlər üçün hazır plaqinlər də mövcuddur (nümunə- Wordpress)

Qeydiyyat zamanı xüsusi mobil tətbiq vasitəsi ilə QR kodu kamera ilə çəkmək kifayətdir. TOTP dəstəkləyən mobil tətbiqlərin sayı 100 yaxındır, istəsəniz özünüz də TOTP tətbiq yarada bilərsiniz.

Kerberos Doğrulama Serveri

İnternet etibarsız bir yerdir. Bəzi sistemlər kompüterlərə icazəsiz girişin qarşısını almaq üçün firewallları yerləşdirir. Lakin təhlükəsizlik duvarları pis adamların kənarda olduğunu düşünür və bu, problemdir. Zərərli cəhdlərin əksəriyyəti daxildən edilir.

Güclü kriptoqrafiyadan istifadə edən Kerberos, etibarsız şəbəkə üzərindən etibarlı hostlar arasında şəbəkə xidməti sorğularının autentifikasiyası üçün protokoldur. O, müştəri-

server proqramlarının yaradılması və istifadəçilərin şəxsiyyətlərinin yoxlanması üçün təhlükəsizlik açarı kriptoqrafiyasından və etibarlı üçüncü tərəfdən istifadə edir.

Kerberos, müştərinin özünü Doğrulama Serverinə (AS) autentifikasiya etdiyi və bileti (Açar Dağıtım Mərkəzi ilə əlaqə arasında iştirak edən müxtəlif addımlar) aldığı bilet mexanizminə əsaslanan autentifikasiya protokoludur ki, o, eyni serverdən istifadə edərək bütün qovşaqlarla təkrar istifadə edə bilər. Beləliklə, daxili şəbəkədə siz özünüzü AS-də autentifikasiya etməklə və sonra digər qovşaqlara daxil olmaq üçün biletdən yenidən istifadə etməklə qovşaqlara daxil ola bilərsiniz.

Kerberos əsasən etibarlı audit və autentifikasiya funksiyalarını tələb edən təhlükəsiz sistemlərdə istifadə olunur. O, ssh, POP və SMTP üçün alternativ autentifikasiya sistemi olan Posix autentifikasiyasında, Active Directory, NFS, Samba və bir sıra digər oxşar layihələrdə istifadə olunur. O, müntəzəm olaraq POSIX autentifikasiyasını başa düşən hər şey üçün açılan sistem kimi istifadə oluna bilər, bu da kifayət qədər azdır.

Kerberos istənilən kibertəhlükəsizlik qurğusuna bir çox üstünlüklər gətirir. Əsas üstünlükləri bunlardır:

- Effektiv giriş nəzarəti: Kerberos istifadəçilərə qiymətli kağızların və giriş siyasətinin icrasını izləmək üçün bir xal verir.
- Kritik biletlər üçün etibarlı ömürlük giriş: Hər bir Kerberos biletində bilet vaxt möhürü, ömürlük data və administrator tərəfindən idarə olunan autentifikasiya qrafiki var.

- On-point identifikasiyası: Bəzi xidmət sistemləri və istifadəçilər qarşılıqlı autentifikasiya vasitəsilə bir-birlərini autentifikasiya edə və istifadə edə bilərlər.
- Yenidən istifadə edilə bilən autentifikasiya: Kerberos autentifikasiyasından istifadə edən hər kəs təkrar istifadə edə bilər və davamlıdır, hər bir istifadəçidən sistem tərəfindən bir dəfə yoxlanılmasını tələb edir. Bilet istifadəyə yararlı olduğu müddətcə istifadəçi autentifikasiya məqsədləri üçün öz məlumatlarını saxlamalı olmayacaq.
- Möhkəm və müxtəlif təhlükəsizlik tədbirləri: Kerberos etibarlı və təhlükəsiz müdafiə yaratmaqla kriptoqrafiya, bir neçə məxfi açar və üçüncü tərəf icazəsi istifadə etmək üçün təhlükəsizlik identifikasiyası mühafizəsinə malikdir. Kerberos ilə əlaqəli bir şey, parolların şəbəkələr üzərindən göndərilməməsi, şəxsi açarların şifrələnməsidir.

Müştəri: Müştəri istifadəçi təcrübəsi adı ilə hərəkət edir və xidmət sorğusu üçün rabitə rolunu oynayır.

server: Server ona daxil olmaq istəyən istifadəçini qəbul edir.

Doğrulama serveri (AS): AS tələb olunan müştəri autentifikasiyasını həyata keçirir. Əgər autentifikasiya uğurla işə salınarsa, müştəri TGT adlı bilet alır ki, bu da əsasən digər müştərilərin serverlərinin autentifikasiya olunduğunun təsdiqidir.

§12. Yeni nəsil elektron rəqəmsal imzalar.

Kriptoqrafiya üsulları təkcə məlumatları məxfiləşdirməyə imkan vermir. Həmçinin, məlumatın tamlığını qorumaq üçün onun dəyişdirilməsi, yaxud mətnin başqası ilə əvəz edilməsi faktını, o cümlədən, məlumatın mənbəyinin həqiqiliyini aşkarlamağa imkan verən üsullar da mövcuddur. Son zamanlar rəqəmli imza texnologiyası meydana çıxmışdır ki, bu da imzalanmış sənədi ancaq kağız şəklində çatdırmaq zərurətini aradan qaldırmışdır.

Mahiyyət etibarilə imza, imzalayanın hər hansı bir sənədin, yaxud müqavilənin məzmununu təsdiq (qəbul) etmə niyyətini əks etdirən işarədir. Tarix boyunca xaç işarəsi, "X", barmaq izi və s. imza kimi istifadə olunmuşdur.

Elektron imza müstəqil imza forması kimi.

Elektron imza, elektron formada olan məlumatlarla bağlı hər hansı razılaşmanı (qəbul etməni) təsdiq etmək üçün işlənir və imza kimi hüquqi qüvvəyə malikdir.

Elektron imza, cəmiyyətdə yaranan münasibətlərdə təhlükəsiz və dəqiq identifikasiya olunan imzalama metodu formalaşdırmaq məqsədilə yaranmışdır. Yurisdiksiyadan asılı olaraq e-imzaya müxtəlif anlayış və izahlar verilir. Gücləndirilmiş elektron imza haqqında müxtəlif dövlətlərin yanaşmalarının ortaq məxrəci aşağıdakı tələbləri müəyyən edir:

- İmza sahibinin kimliyi və imza ilə bağlılığı müəyyənləşdirilib təsdiq edilməlidir;
- Imza sahibi imzadan istifadə üçün yaradılan yeganə gizli elektron açardan (giriş kodu) yalnız özü istifadə etməlidir[3];

- Imza, razılaşdırılmış məlumatın imzalanmadan sonra təhrif olunması halını müəyyənləşdirmək imkanına malik olmalıdır;
- İmzalanmış məlumatın dəyişdirilməsi hallarında imza etibarsız sayılır.

Zaman keçdikcə, rəqəmsal imzadan e-kommersiya əməliyyatları və tənzimləmə sənədləşdirmələrində elektron imzanın qorunan zahiri forması kimi geniş istifadə olunmağa başlanılmışdır. Beynəlxalq, eləcə də bir sıra milli standartlaşdırma qurumları elektron imzanı standartlaşdırmaqla tətbiqini daha da asanlaşdırmağa çalışır (bax NİST, ETSİ).

E-imzaları daha xüsusi şəkildə aşağıdakı kimi kateqoriyalaşdırmaq olar:

- "Click to sign" – işarə xanalarından, skan edilmiş və yazılmış adlardan ibarət olur. Bu üsul imzalayanın kimliyini sübut etmək, imzalanmış verilənləri dəyişiklərdən qorumaq üçün yaxşı vasitə hesab olunmur. Onlar daha çox digər e-imza və rəqəmsal imzalarla birlikdə istifadə olunur.
- "e-imzalar"- Bu qaydaya əsasən imzalayan öz imzasının əlyazma formasını rəqəmsal kriptoqrafik qorunan (elektron) formada sənədə əlavə edir.
- "Advanced and Qualified eSignatures"- "Gücləndirilmiş elektron imza" yuxarıda da qeyd olunduğu kimi AB tərəfindən müəyyən edilmiş bütün əsas tələblərə cavab verən imzalardır. Bu imzaların ən üstün cəhəti imza sahibinin dəqiq şəkildə göstərilməsidir.

Elektron imzalar bir sıra dövlətlərin qanunvericiliyində ya ümumi ya da birbaşa e-imzalara ayrılmış xüsusi

normalar ilə tənzimlənir. Türkiyə, Yaponiya və Ukraynanın sırf e-imzaya həsr olunmuş ayrıca qanunları, ABŞ-ın isə bununla bağlı müxtəlif məsələləri tənzimləyən 5 normativ hüquqi sənədi qüvvədədir. Avstraliya və Yeni Zellandiyanın isə Elektron əqdlər haqqında Aktları (ardıcıl olaraq 1999 və 2002) qəbul olunmuşdur.

Azərbaycan Respublikası qanunvericiliyində də elektron imzalara xüsusi qanun həsr olunmuşdur. (Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının qanunvericiliyi Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu ilə yanaşı Azərbaycan Respublikasının Konstitusiyasından, Azərbaycan Respublikasının tərəfdar çıxdığı beynəlxalq müqavilələrdən, Azərbaycan Respublikasının Mülki Məcəlləsindən, bu qanundan, "Dövlət sirri haqqında", "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının qanunlarından və digər normativ hüquqi aktlardan ibarətdir.)

Müasir dövrdə elektron əqdlərin ictimai münasibətlərin ayrılmaz parçası olduğunu və əhəmiyyətinin getdikcə artdığını nəzərə alaraq elektron imzanı da bu sürətlə yayılma prosesinin başlıca iştirakçısı hesab edə bilərik.

Rəqəmli imza dedikdə, aydındır ki, söhbət imzanın skaner vasitəsilə üzünün çıxarılmasından getmir. Rəqəmli imza, yaxud elektron imza şəxsi gizli şifrdir və onun açarı yalnız onun sahibinə məlumdur. Rəqəmli imza üsullarında çox zaman asimmetrik şifrləmə alqoritmlərindən – şifrləmə üçün gizli açardan, deşifrləmə üçün isə açıq açardan istifadə olunur. Rəqəmli imza məlumatın həqiqiliyinin imza sahibi tərəfindən təsdiq olunduğunu bildirir. Əgər

rəqəmli imza ilə təsdiq olunmuş sənəd almısınızsa, onda sizə şifri açmaq üçün imza sahibinin vermiş olduğu açıq açar da lazımdır.

Rəqəmli sertifikat səlahiyyətli orqan tərəfindən imzalanmış elə məlumatdır ki, orada açıq açarın həqiqətən də, imza sahibinə aid olması və deşifrləmə məqsədilə istifadə oluna bilməsi təsdiqlənir. Sertifikatlaşmaya səlahiyyəti olan orqandan sertifikat almaq üçün həmin orqana ərizəçinin kimliyi ilə bağlı müxtəlif sənədlər təqdim olunmalıdır.

Elektron sənədləri ilə mübadiləni yerinə yetirdikdə alınmış sənədin müəllifinin, onun doğru olub-olmamasını və informasiyanın bütöv olmasının quraşdırılması vacib əhəmiyyət kəsb edir. Bu cür məsələnin həlli elektron sənədini müşayiət edən rəqəmsal imzanın üzərinə düşür. Funksional cəhətdən o, adi əl ilə çəkilən imza ilə analoji olur və onun aşağıdakı əsas üstün cəhətlərinə malik olur:

1) təsdiq edir ki, imzalanmış mətn onu imza edən şəxsə məxsusdur;

2) mətnə imza atan şəxsə imzalanmış mətn ilə əlaqəli olan öhdəliklərdən boyun qaçırmağa imkan vermir;

3) imzalanmış mətnin bütövlüyünə zəmanət verir. Elektron rəqəmsal imza sənəd ilə birlikdə ötürülən nisbətən çox da böyük olmayan əlavə informasiya deməkdir.

Adətən rəqəmsal imza açıq açar üsulunun tətbiq olunması ilə şifrlənir və məzmunu, imzanın özünü və bir cüt açarları əlaqələndirir. Bu elementlərdən heç olmazsa birinin dəyişdirilməsi rəqəmsal imzanın doğruluğunu təsdiq etməyə iman vermir. Rəqəmsal imzanın formalaşması mərhələsində məxfi və açıq açar kimi iki açar generasiya olunur. Açıq açar elektron sənədinin

göndərildiyi bütün abonentlərə paylaşdırılır.

Sənədə əlavə olunan imza məktub göndərənin aşağıdakı parametrlərinə malik olur: imza tarixi, məktub göndərən barəsində informasiya və açıq açarın adı. Bütün sənədə tətbiq edilən xeş-funksiyanın köməkliyi ilə bütövlükdə bütün mətni xarakterizə edən çox da böyük olmayan ədəd hesablanır. Bu ədəd sonra məxfi açarla şifrlənir və elektron rəqəmsal imza rolunu oynayır.

Məktub alana açıq şəkildə sənədin özü və elektron imza göndərilir. Yoxlama zamanı məktub alana məlum olan açıq açarla rəqəmsal imzanın şifri açılır. Əldə edilmiş açıq sənədə xeş-funksiya çevirməsi tətbiq edilir. Onun işinin nəticəsi göndərilmiş elektron imza ilə müqayisə edilir. Əgər hər iki ədəd üst-üstə düşərsə, o zaman əldə edilmiş sənəd həqiqi olacaqdır.

Aydındır ki, sənədə istənilən icazə verilməmiş dəyişiklik edilməsi açıq sənəd üzrə hesablanan xeş-funksiyanın qiymətinin dəyişilməsinə gətirib çıxaracaqdır, amma məxfi açarla şifrlənmiş elektron imzanı başqası ilə əvəz etmək cinayətkar üçün çox çətin olacaqdır.

Elektron imza sistemi elektron imza vasitələrinin köməyi ilə aşağıdakı iki proseduranı özündə birləşdirir:

- elektron imzanın yaradılması;
- elektron imzanın yoxlanılması.

Asan İmza ilə şəxsiyyət vəsiqəsini təqdim etmədən kimliyinizi təsdiq edə, eyni zamanda mobil telefondan istifadə edərək sənədləri elektron qaydada imzalaya bilərsiz. Yəni, sənədlərə rəqəmsal imza ata bilərsiz. Asan İmza (Mobil imza) ilə bütün mövcud e-xidmətlərdən istifadə etmək mümkündür.

Asan İmza ilə hökumət vətəndaş arasında bürokratik

əngəlləri aradan qaldırmaq olur. Bu, o deməkdir ki, Azərbaycan hökuməti telefon vasitəsilə hər zaman öz vətəndaşları ilə birlikdədir.

Asan İmza (Mobil imza) əslində elektron mühitdə fiziki İD-karta bərabər sənəd kimi sertifikatlara bağlı olan mobil telefon SİM-kartınızdır.

Qeyd edək ki, Asan İmza Vergilər Nazirliyi və Mobil operator tərəfindən verilir. Asan İmza xidmətindən istifadə etmək üçün Asan İmza Sim kartını əldə etmək lazımdır. Abunəçi olmaq üçün şəxsiyyət vəsiqəniz ilə (şəxsiyyət vəsiqəsi Asan İmza (Mobil imza) xidmətini aktivləşdirmək üçün lazımdır) ―ASAN Xidmət‖ mərkəzində fəaiyyət göstərən Azercell ofisinə, Azercell Ekspres və Müştəri Xidmətləri ofislərinə (yaxın gələcəkdə isə digər mobil operatorların ofislərinə) müraciət edə bilərsiniz. Abunəçi olandan sonra siz mobil telefona daxil edilməli olan yeni Asan İmza (Mobil imza) SIM kartını alacaqsınız. Sonrakı mərhələdə tələb olunan sənədlər ilə birlikdə ASXM (Vergi ödəyicilərinə Xidmət Mərkəzlərinə, Bakı şəhər Vergilər Departamentinə.

Asan İmza (Mobil imza) PIN kodları Asan İmza (Mobil imza) SIM kartının üzərində çap olunaraq, pozulan qat altında gizlədilir. Yeni Asan İmza (Mobil imza) SIM kartının pozulan sahəsi zədələnməməlidir. Yadda saxlayın ki, şəxsiyyətin təsdiqlənməsi üçün PIN1 və imza üçün yalnız PIN2 tələb olunur. Asan İmza (Mobil imza) elektron imza sertifikatlarının üç növü vardır: fiziki şəxslər (vətəndaşlar) üçün elektron imza sertifikatları, hüquqi və sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxslər üçün və dövlət qulluqçuları üçün elektron imza sertifikatları.

Fiziki şəxslər (vətəndaşlar) üçün elektron imza

sertifikatları şəxsi istifadə üçün nəzərdə tutulub. Siz bu sertifikatdan yalnız şəxsi identifikasiyanız üçün istifadə edə bilərsiniz. Hüquqi şəxslər və sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxslər, həmçinin dövlət qulluqçuları üçün nəzərdə tutulan elektron imza sertifikatları isə kommersiya və ya dövlət təşkilatını təmsil etmək və onun adından çıxış etmək səlahiyyətləri verir.

Qeyd edək ki, Asan İmza (Mobil imza) sertifikatları 3 il ərzində etibarlıdır. Asan İmza (Mobil imza) xidmətinin istifadəsi pulludur. Xidmətlərin qiymət siyahısı sizin mobil operatorunuzun internet səhifəsində mövcuddur: Azercell, Bakcell, Nar Mobile.

SİMA İmza – bulud, açıq açar və üztanıma texnologiyalarına əsaslanan yeni nəsil gücləndirilmiş rəqəmsal imzadır. Mobil tətbiq əsaslı SİMA İmza əlavə vasitələrə ehtiyac olmadan, istənilən yerdən və istənilən zaman daha rahat şəkildə elektron xidmətlər əldə etməyə imkan verir.

"SİMA İmza" Azərbaycan Respublikasının vətəndaşları, fərdi sahibkarları tərəfindən istifadə olunur.

"SİMA İmza" həm vətəndaşlar, həm də xidmət təklif edənlər üçün bir sıra üstünlüklər yaradır. Yeni nəsil rəqəmsal imza ilə maliyyə xərcləri azalır, vaxt itkisi aradan qalxır. Həmçinin "SİMA İmza"nın istənilən sistemə inteqrasiya oluna bilməsi, eləcə də avtomatlaşdırma istifadəçilərə sürətli və istənilən sayda imzalama imkanı qazandırır. Vətəndaşların bu imkanlardan faydalanmaq üçün "SİMA İmza" tətbiqini mobil cihaza yükləməsi və bir dəfə qeydiyyatdan keçməsi kifayətdir.

"SİMA İmza"nın vətəndaşlar üçün tam pulsuz olması, heç yerə getmədən cəmi 1 dəqiqə ərzində mobil tətbiqdə

qeydiyyatdan keçərək əldə olunması, imzanı əldə etmək üçün tək şəxsiyyət vəsiqəsinin kifayət etməsi vətəndaşlar kimi bankların da iş yükünü azaldır, vaxta və xərcə qənaət etmək üçün zəmin yaradır.

"SİMA İmza"nın maliyyə əməliyyatları zamanı tərəfdaşlarına qazandırdığı ən mühüm üstünlük isə imzanın etibarlılığıdır. Hüquqi olaraq əl imzasına bərabər tutulan "SİMA İmza" üztanıma texnologiyasına əsaslandığı üçün bir şəxsin "SİMA İmza"sı ilə başqa bir şəxsin imza etməsi mümkünsüzdür.

Rəqəmsal xidmətlərə əlçatanlığı artıran "SİMA İmza" ölkəmizdə biznes proseslərini sürətləndirəcək. Bu rəqəmsal imza bank və bank olmayan kredit təşkilatlarının, sığorta şirkətlərinin, GSM operator, dövlət və özəl qurumlarının xidmətlərindən istifadə zamanı tətbiq edilir.

"SİMA İmza" Azərbaycan Respublikasının "Elektron imza və elektron sənəd haqqında", "Biometrik informasiya haqqında" qanunlarına və Nazirlər Kabinetinin "Azərbaycan Respublikasında elektron imza və elektron sənədlə bağlı bəzi normativ hüquqi aktların təsdiq edilməsi haqqında" qərarına tam uyğundur.

SİMA Token – beynəlxalq təhlükəsizlik standartına uyğunlaşdırılmış, virtual məkanda şəxsiyyəti müəyyənləşdirmə məqsədi üçün istifadə edilən gücləndirilmiş elektron imzadır. Azərbaycan Respublikasının mövcud qanunvericiliyinə əsasən, gücləndirilmiş elektron imza ilə imzalanan elektron sənədlər əl imzası ilə imzalanan və möhürlənən sənədlərə bərabər tutulur.

§13. Əməliyyat sistemlərinin təhlükəsizliyinin təmin edilməsi

Əksər informasiyanın proqram müdafiə vasitələrinin çoxu tətbiqi proqramlardır. Onların yerinə yetirilməsi üçün mütləq Əməliyyat sistemindən (ƏS) dəstək lazımdır. Əməliyyat sistemlərinə məxsus olan funksiyaların yerinə yetirilməsinin əhatə dairəsi etibarlı hesablama bazası (EHB) adlanır. Etibarlı hesablama bazası informasiya təhlükəsizliyini təmin edən elementlər toplumundan ibarətdir. Bura proqramlar, şəbəkə avadanlıqları, vəsaitlərin fiziki müdafiəsi və təşkilatı prosedurlar daxildir. Əmələ gələn piramidanın əsas müdafiəsi əməliyyat sistemidir.

Əməliyyat sisteminin effektiv və etibarlı müdafiəsinin təşkili mümkün hədələrin və onların təhlükəsizliyinin öncədən təhlili olmadan mümkün deyil. Əməliyyat sistemlərinin hədələrdən təhlükəsizliyi sistemin istimar şərtlərindən, hansı informasiyanın yaddaşda saxlanılmasından, hansı informasiyanın sistemdə təhlil edilməsindən və buna bənzərlərdən hiss ediləcək dərəcədə asılıdır. Məsələn, əgər əməliyyat sistemi müəssisədə elektron sənəd dövriyyəsi üçün istifadə edilirsə, onda ən təhlükəli hədə qeyriqanuni əlçatanlığın fayllara vurduğu ziyandır. Əgər əməliyyat sistemi İnternet-xidmətin provayder platformasinda istifadə edilirsə, onda ən qorxulu hücumlar əməliyyat sisteminin şəbəkə proqram təminatına edilən hücumlardır.

Əməliyyat sistemlərinin hədələrdən təhlükəsizliyini onların istifadə edilmə baxımından təsnifləşdirmək olar.

1. Hücumun məqsədinə görə:

- İnformasiyanın qeyriqanuni oxunmasına görə;
- İnformasiyanın qeyriqanuni dəyişdirilməsinə görə;
- İnformasiyanın qeyriqanuni məhv edilməsinə görə;
- Əməliyyat sisteminin tam və ya hissə-hissə dağılmasına görə.

2.Əməliyyat sisteminə təsir prinsipinə görə:

- İnformasiyanın əldə edilməsi üçün məşhur (leqal) kanallardan istifadə edilməsi, məsələn, faylların qeyriqanuni oxunmasına hədələr və s.;
- İnformasiyanın əldə edilməsi üçün gizli kanalların istifadə olunması, məsələn, bədniyyətli insanın əməliyyat sisteminin sənədləşdirilməmiş imkanlarından istifadə etmək üçün hədələrdən istifadə etməsi;
- Proqram əlavələrinin köməyilə informasiyanın əldə edilməsi üçün yeni kanalların yaradılması.

3.Bədniyyətli insan tərəfindən müdafiənin pis vəziyyətə salınması növünə görə:

- Uyğun olmayan təhlükəsizlik siyasəti, o cümlədən sistem inzibatçısının səhvləri;
- Əməliyyat sisteminin səhvi və proqram təminatı imkanlarının sənədləşdirilməməsi, o cümlədən sistemin müdafiəsini yan keçməyə imkan verən, təsadüfən və ya düşünülmüş şəkildə qurulan "xidməti giriş" (onu çox vaxt "lyuk – anbar ağzı" da) adlandırırlar;
- Əvvəllər istifadə olunan proqram əlavələri.

4.Əməliyyat sisteminə etdiyi təsirin xarakterinə görə:

- Aktiv təsir – pisniyyətli insanın sistemə qeyriqanuni təsir göstərməsi;

- Passiv təsir – sistemdə baş verən proseslərin eyriqanuni şəkildə pisniyyətli insan tərəfindən müşahidə edilməsi.

Əməliyyat sisteminin təhlükəsizlik hədələrini onların əlamətlərinə görə təsnif edirlər. Bunlara: pisniyyətli insan tərəfindən edilən təsirin üsulu, istifadə edilən hücum vasitələri, hücum obyektləri, hücuma məruz qalan obyektə edilən təsirin üsulları, hücum edilən obyektdə istifadə edilən əməliyyat sisteminin hücum zamanı vəziyyəti aiddir.

Əməliyyat sistemi aşağıdakı hücumlara məruz qala bilər:

- Fayl sisteminin skanerə edilməsi. Bədniyyətli insan kompüterin fayl sisteminə nəzər salır və bütün faylları ardıcıl oxumağa (və ya surətini almağa) cəhd göstərir. Gec və ya tez inzibatçının heç olmasa bir səhvi aşkar olunur. Nəticədə pisniyyətli insan ona qadağa qoyulmuş informasiyaya əlçatanlıq edir;
- Parolun seçilməsi. Parolun seçilməsində bir neçə üsuldan istifadə edilir:
- Ümumi izafə (izafə - normadan artıq alınmış (götürülmüş) şey anlamını verir);
- Statistikada rast gəlinən simvolların optimallaşdırılması və ya lüğətdan istifadə etməklə ümumi izafə;
- İstifadəçini tanımaqla parolun seçilməsi (onun adı, soyadı, doğum günü, telefon nömrəsi və s.);
- Açar informasiyanın oğurlanması. Pisniyyətli insan istifadəçi tərəfindən yığılmış parola baxa bilər və yaxud da, istifadəçının klaviatura üzərində əlinin hərəkətini izləməklə onun yığdığı parolu bərpa edə bilər. Bununla yanaşı açar informasiya (smart-kart,

Touch Memory və başqaları) pisniyyətli insan tərəfindən sadəcə oğurlana bilər;

- "Zibil qutu"suna atılmışın toplanması. Bir çox əməliyyat sistemlərində stifadəçi tərəfindən ləğv edilmiş informasiya fiziki olaraq ləğv olunmur, sadacə olaraq "Zibil qutusu" adlanan qutuya atılır. Bədniyyətli insan atılmış informasiyanı bərpa edir, ona baxış keçirir və ona lazım olan hissələrin (ola bilsin tam faylın) surətini alır;
- Səlahiyyətini aşma. Bədniyyətli insan əməliyyat sistemində proqram təminatındakı səhvdən və təhlükəsizlik siyasətindən istifadə etməklə özü üçün səlahiyyət əldə edir. Adətən belə hallar proqramı işə salarkən başqa istifadəçinin adından istifadə etdikdə baş verir;
- Proqrama qoşulma. Əməliyyat sistemlərində istifadə olunan proqrama qoşulma digər proqrama qoşulmalar sinifindən fərqlənmir;
- Proqrama acgözlük. Bu proqram kompüterin bəzi resurslarını ələ keçirə bilir, nəticədə digər proqramlar ya yerinə yetirilə bilmirlər, ya da ki, ağır sürətlə yerinə yetirilirlər. Acgöz proqramın işə salınması məhvə gətirib çıxarır.

Əməliyyat sisteminin müdafiə olunma anlayışı

Əməliyyat sistemi o vaxt müdafiə olunan sayılır ki, o kanardan edilən müxtəlif sinif hücumları dəff edə biləcək vasitələrdən istifadə edə bilsin. Müdafiə olunan əməliyyat sistemi mütləq şəkildə istifadəçinin onun resurslarına əlçatanlıq etməsinə məhdudiyyət qoyan vasitələrə malik olmalıdır. Bununla yanaşı əməliyyat sistemində istifadəçinin həqiqiliyini yoxlaya biləcək vəsaitdə

olmalıdır. Əməliyyat sistemi təsadüfi təsirlərə və ya onun işini pozacaq (işdən çıxara biləcək) hallara da hazır olmalıdır.

Bəzən elə olur ki, əməliyyat sistemi bütün baş verə biləcək hədələrdən deyil, onlardan bəzilərindən müdafiə olunur. Belə olan halda əməliyyat sistemi qismən müdafiə olunan əməliyyat sistemi adlandırılır.

Əməliyyat sisteminin müdafiə olunmasına yanaşma

Əməliyyat sisteminin müdafiə edilməsinə iki əsas yanaşma mövcuddur–fraqmentlərlə və kompleks. Fraqmentlərlə yanaşmada əvvəlcə bir hədədən müdafiəni həyata keçirirlər, sonra növbəti hədəni və s. Fraqmentlərlə yanaşmaya nümunə kimi müdafiə edilməyən Windows 98 əməliyyat sistemini göstərmək olar, çünki, əməliyyat sisteminə antivirus proqramı quraşdırılır, şifrələmə sistemindən istifadə edilir, istifadəçinin fəaliyyəti qeydiyyat sistemində nəzərədə saxlanılır və s.

Fraqmentlərlə yanaşmada əməliyyat sisteminin altsisteminin müdafiə edilməsi dedikdə müxtəlif istehsalçılardan alınan dağınıq proqram məhsulları nəzərədə tutulur. Bu proqram vasitələri bir-birindən asılı olmadaq işləyirlər (iş zamanı onların birliyini təmin etmək praktiki olaraq mümkün deyil). Bununla yanaşı belə altsistemin müdafiə edilməsinin ayrı-ayrı elementləri bir-biri ilə kobudcasına (qeyrikorrekt) işlədiyinə görə ümumilikdə sistemin etibarlığı sərt şəkildə aşağı düşür.

Kompleks yanaşmada müdafiə funksiyası əməliyyat sistemi layihələndirilmə mərhələsində olanda ona daxil edilir və onun ayrılmaz hissəsinə çevrilir. Kompleks yanaşmaya əsaslanaraq yaradılmış altsistemin müdafiə olunmasının ayri- ayri elementləri müxtəlif məsələlərin

həll edilməsində və informasiyanın müdafiə edilməsində bir-birilə qarşılıqlı əlaqədə olduğu üçün ayrı-ayrı elementlər arasında praktiki olaraq münaqişənin yaranması mümklün deyil.

Kompleks yanaşma əsasında qurulmuş altsistemin müdafiəsi bəzən elə qurulur ki, sistemdə qarşısı alınmaz pozuntular baş verdikdə əməliyyat sisteminin əsas elementlərində yaranan bu hallar (pozuntular) əməliyyat sisteminin müvəffəqiyyətsizliyinə gətirib çıxarır, nəticədə pisniyyətli insan sistemin müdafiə olunma funksiyasını pozmağa imkan tapa bilmir. Nəzərə almaq lazımdır ki, fraqmentlərlə yanaşmada altsistemin bu şəkildə müdafiə edilməsi mümkün deyil.

Müdafiənin inzibati tədbirləri

Əməliyyat sisteminin müdafiəsinin proqram-aparat vasitələri mütləq inzibatı tədbirlər ilə tamamlanmalıdır. İnzibatçı tərəfindən daim ixtisaslaşdırılmış dəstək yerinə yetirilməsə ən etibarlı proqram-aparat müdafiəsi belə nəticəsiz alına bilər.

Aşağıda əsas inzibatı tədbirlər verimişdir:

1.Əməliyyat sisteminin daim işlək olmasına nəzarətin korrektliyi xüsusilə onun altsisteminin müdafiəsi ilə bağlıdır. Belə nəzarəti təşkil etmək əlverişlidir. Bu əsasən o zaman baş verir ki, əməliyyat sistemi əsas hadisələrin (event logging) xüsusi jurnalda avtomatik olaraq qeyd olunmasını dəstəkləyir.

2. Adekvat (tam uyğun) təhlükəsizlik siyasətinin təşkili və dəstəklənməsi. Əməliyyat sisteminin təhlükəsizlik siyasəti daim korrektə edilməlidir, çünki bədniyyətli insan əməliyyat sisteminə ziyan vura bilər, onun quruluşunu dəyişər, tətbiqi proqramların qurulmasına və

ya sistemdən kanarlaşdırılmasına maneçilik edə bilər.

3.İstifadəçinin əməliyyat sistemindən istifadəsinin təlimatlandırılması əməliyyat sisteminin işlədiyi zaman ərzində təhlükəsizlik tədbirlərinə riayət edilməsinə və bu tədbirlərin həyata keçirilməsinə nəzarətin yerinə yetirilməsinə imkan verir.

4.Mütamadi olaraq ehtiyat surətlərin və əməliyyat sistemi verilənlərinin yaradılması və təzələnməsi.

5.Əməliyyat sisteminin, verilənlərin təhlükəsizlik siyasətinin və quruluşunun dəyişməsinə daim nəzarət.

Belə dəyşiklikləri qeyrielektrik informasiya insanın əməliyyat sisteminin müdafiəsini dağıdaraq sistemə daxil olması və özünü maskalayaraq qeyriqanuni fəaliyyət göstərməsi mümkün olmaz.

Adekvat təhlükəsizlik siyasəti

Adekvat təhlükəsizlik siyasətinin seçilməsi və dəstəklənməsi əməliyyat sistemi inzibatçısının əsas vacib məsələlərindən biri sayılır. Əgər əməliyyat sistemində qəbul olunmuş təhlükəsizlik siyasəti adekvat deyilsə, bu pisniyyətli insanın sistemin resurslarına qeyriqanuni əlçatanlığına imkan verəcək və əməliyyat sisteminin etibarlı işləməsinə şərait yaradacaq.

Məlumdur ki, əməliyyat sıstemi nə qədər yaxşı müdafiə olunarsa, istifadəçinin və inzibatçının onunla işləməsi bir o qədər çətin olacaqdır. Bu aşağıdakı faktorlar ilə bağlıdır:

- İstifadəçinin bəzi əməllərinin qərəzli olduğunu müdafiə sistemi həmişə müəyyən edə bilmir. Sistem nə qədər çox müdafiə olunarsa, istifadəçinin leqal fəaliyyəti bir o qədər yüksək olacaqdır;
- İstənilən sistemdə informasiyanın müdafiə funksiyası nəzərə alınmışsa, inzibatçıdan adekvat təhlükəsizlik

siyasətinin dəstəklənməsinə istiqamətlənmiş müəyyən fədakarlıq tələb edilir. Əməliyyat sistemində müdafiə funksiyası nə qədər yüksək olarsa, müdafiənin dəstəklənməsi üçün bir o qədər vaxt və vəsait tələb olunur;

- Əməliyyat sistemi müdafiəsinin altsistemi, həmçinin istənilən başqa bir proqram paketi kompüterin aparat vasitələrinin resurslarını sərf edir. Əməliyyat sisteminin müdafiə funksiyası nə qədər mürəkkəb qurularsa, kompüterin resursları da bir o qədər çox olacaqdır (məsələn, prosessor vaxtı, operativ yaddaş və s.). Bu resurslar müdafiə altsisteminin dəstəklənməsinə sərf edilir və kompüterin tətbiqi proqramına bir o qədər az resurs payı düşür;
- Təhlükəsizlik siyasətinin həddidən artıq dəstəklənməsi əməliyyat sisteminin işləməsinə neqativ təsir edə bilər. Siyasətə həddindən artiq sərt yanaşma çətin aşkarlanan səhvlərə səbəb ola bilir və əməliyyat sisteminin işini dayandırmasına, nəticədə məhv olmasına gətirib çıxarır;
- Təhlükəsizlik siyasətinin optimal adekvatlığı dedikdə bədniyyətli insana nəin ki, qeyriqanuni fəaliyyətini həyata keçirməyə imkanın verilməməsi, həmçinin öndə yazılanlarda neqativ effektin baş verməsinə gətirib çıxarmaması prosesi başa düşülür.

Adekvat siyasət nəin ki, əməliyyat sisteminin arxitekturası ilə müəyyən edilir, həm də ki, onun quruluşu, ona quraşdırılmış tətbiqi proqramlar və i.a. ilə müəyyən edilir. Əməliyyat sisteminin adekvat təhlükəsizlik siyasətinin formalaşmasını və dəstəklənməsini iki mərhələyə bölürlər.

1.Hücumların təhlili. Əməliyyat sisteminin administratoru

əməliyyat sisteminin cari nüsxəsində mümkün təhlükəsizlik hədələrinə (hücumlarına) baxış keçirir. Mümkün hədələrin içərisindən ən çox təhlükəli olanları seçilir və onlardan müdafiə üçün maksimum vəsait ayrılır.

2. Təhlükəsizlik siyasətinə tələbin formalaşdırılması. Bu və ya digər hədələrdən müdafiə olunmaq üçün hansı üsullardan və vəsaitlərdən istifadə edilməsini administrator (inzibatçı) müəyyən edir. Məsələn, əməliyyat sisteminin bəzi obyektlərinin qeyriqanuni əlçatanlıqdan müdafiə olunması üçün müxtəlif üsullardan – kriptoqrafik vasitələrdən, əlçatanlıqla mübarizə apara bilən bəzi vasitələrin kombinasiyalarından və s. istifadə olunur.

3. Təhlükəsizlik siyasətinin formal müəyyən edilməsi. İnzibatçı öndəki mərhələdə formalaşdırılmış tələblərin konkret olaraq necə yerinə yetirilməsini müəyyən edir. Əməliyyat sisteminin quruluşuna, həmçinin əlavə müdafiə paketlərinə olan tələblər formalaşdırılır. Formalaşdırma əməliyyatı ancaq belə paketlərin qurulmasına ehtiyac duyulduqda həyata keçirilir. Yerinə yetirilmiş mərhələnin nəticəsi əməliyyat sisteminin konfiqurasiyasının qurulmasını açıq şəkildə əks etdirən siyahısının tərtib edilməsi və hansı vəziyyətdə hansı sazlamanın qurulması üçün əlavə müdafiə paketlərindən istifadə edilməsi ilə bağlıdır.

4. Təhlükəsilik siyasətinin həyata keçirilməsi. Bu mərhələnin məqsədi öndəki mərhələdə formal olaraq müəyyən edilmiş əməliyyat sisteminin konfiqurasiyasının və əlavə müdafiə paketlərinin təhlükəsizlik siyasətinə uyğun həyata keçirilməsidir.

5. Təhlükəsizlik siyasətinin korreksiya olunması və

dəstəklənməsi. Bu mərhələdə inzibatçının qarşısında duran əsas məsələ təhlükəsizlik siyasətinə nəzarəti yerinə yetirmək və lazım gəldikdə müəyyən dəyişiklikləri həyata keçirməkdir.

Qeyd etmək lazımdır ki, əməliyyat sisteminin müdafiə edilməsi üçün xüsusi olaraq hazırlanmış standart hələlik yoxdur. Əməliyyat sisteminin müdafiə edilməsini qiymətləndirmək üçün ümumilikdə kompüter sistemi üçün işlənib hazırlanmış standartdan istifadə edilir.

Adətən əməliyyat sisteminin sertifikatlaşdırılması adekvat təhlükəsizlik siyasəti üçün tələblərin tərtib edilməsi ilə müşahidə olunur. Adekvat təhlükəsizlik siyasətini müəyyən edən zaman əməliyyat sisteminin administratoru ilk növbədə əməliyyat sisteminin konkret hədələrdən müdafiə edilməsinə əsaslanmalıdır.

Əməliyyat sisteminin müdafiə altsistemi

Əməliyyat sisteminin müdafiə altsistemi əsasən aşağıdakı funksiyaları yerinə yetirir.

1.İdentifikasiya və autentufikasiya. Heç bir istifadəçi özünü identifikasiya etməmiş əməliyyat sistemi ilə işə başlaya bilməz. İstifadəçi işə başlayan zaman sistemə autentifikasiya olunmuş informasiyanı təqdim etməlidir. Bununla yanaşı istifadəçi sistemə onun varlığını (yəni bu doğurdan da həmin istifadəçidir) təsdiq edəcək informasiyanı da təqdim etməlidir.

2.Məhdudlaşdırılmış əlçatanlıq. Hər bir istifadəçinin əməliyyat sisteminin o obyektlərinə əlçatanlığı olur ki, ona cari təhlükəsizlik siyasəti həmin obyektlərə əlçatanlığa icazə verir.

3.Audit. Əməliyyat sistemi sistemin təhlükəsizliyini dəstəkləyən potensial qorxulu xüsusi hadisələr jurnalına

reaksiya verir.

4.Təhlükəsizlik siyasətinin idarə edilməsi. Təhlükəsizlik siyasəti daim adekvat vəziyyətdə saxlanılmalıdır, yəni əməliyyat sisteminin işləməsi şərtlərinin dəyişməsinə çevik reaksiya verməlidir. Təhlükəsizlik siyasətinin idarə edilməsi sistem administratoru (inzibatçı) tərəfindən həyata keçirilir, administrator bunun üçün uyğun əməliyyat sisteminə qurulmuş vəsaitlərdən istifadə edir.

5.Kriptoqrfaik funksiyalar. İnformasiyanın müdafiə olunmasını kriptoqrafik vəsaitlərdən istifadə etmədən təsəvvür etmək mümkün deyil. Əməliyyat sistemlərində şifrələmə istifadəçinin parollarını və sistemin təhlükəsizliyini, həmçinin qorxulu olan digər verilənləri rabitə kanalları vasitəsilə ötürülməsi və saxlanması zamanı istifadə olunur.

6.Şəbəkə funksiyaları. Müasir əməliyyat sistemləri lokal və ya qlobal kompüter şəbəkələrin tərkibində izolə edilməmiş işləyirlər. Bir şəbəkəyə daxil olan kompüterlərin əməliyyat sistemləri müxtəlif məsələlərin həll edilməsində bir-birinin arasında qarşılıqlı əlaqədə olurlar (o cümlədən, o məsələlərin həllində ki, onlar birbaşa informasiyanın müdafiəsi ilə əlaqəlidirlər).

Müdafiənin altsistemi adətən vahid proqram moduluna malik deyil. Bu baxımdan sadalanmış müdafiə altsisteminin funksiyası bir və ya bir neçə proqram modulu ilə həll olunur. Bəzi funksiyalar bilavasitə əməliyyat sisteminin nüvəsinə quraşdırılırlar (yapışdırılırlar). Odur ki, modullar arasında dəqiq interfeys olmalıdır və bu interfeysdən ümumi məsələlərin həll edilməsində (modulların qarşılıqlı əlaqəsi yaranan zaman) istifadə edilir.

Belə əməliyyat sisteminə Windows əməliyyat sistemini nümunə göstərmək olar. Burada müdafiənin altsistemi əməliyyat sisteminin ümumi arxitekturasında dəqiq seçilir (ayrılır). Amma UNIX əməliyyat sistemində müdafiə funksiyası praktiki olaraq əməliyyat sisteminin bütün elementlərinə paylanmışdır. Qeyd etmək lazımdır ki, istənilən əməliyyat sistemi standart müdafiəni təmin edirsə, onda həmin əməliyyat sistemi öndə sadalanan funksiyaları yerinə yetirməlidir. Adətən əməliyyat sisteminin müdafiə altsistemi proqram modulunun əlavə genişlənməsinə sazlanmış olur.

Obyektə əlçatanlıq metodu

Əməliyyat sisteminə daxil olma imkanı təkcə əməliyyat sisteminin arxitekturası ilə deyil, cari təhlükəsizlik siyasəti ilə də müəyyən olunur. Daxilolma obyektləri kimi avadanlıq resursları (məsələn, prosessor, yaddaşın seqmentləri, disklər və yaddaş lentləri), proqram resursları (məsələn, fayllar, proqramlar, semaforlar), və nəhayət, nə varsa, onlara daxil olma həmişə nəzarətdədir. Hər bir obyekt özünəməxsus unikal ada malikdir, bu adlar sistemdəki digər obyektlərdəki adlardan fərqlənirlər və onlardan hər biri yaxşı müəyyən edilmiş və əhəmiyyəti olan əməliyyatlara daxil ola bilir.

Obyektə əlçatanlıq metodu obyekt üçün müəyyən olunmuş əməliyyat adlanır. Əməliyyatın növü obyektdən asılıdır. Məsələn, prosessor əmr yerinə yetirir, yaddaş seqmentləri yazılır və oxuna bilir, maqnit disk hesablayıcıları ancaq oxuya bilir, fayllar üçün "oxumaq" və "əlavə etmək" (faylın sonuna informasiya əlavə etmək nəzərdə tutulur) üçün əlçatanlıq metodu müəyyən edilir və s.

Subyektə əlçatanlıq obyekt üzərində əməliyyatı yerinə yetirməyə imkanı olan (obyektə bir neçə əlçatanlıq üsulu ilə müraciət edə bilən), təşəbbüs göstərə bilən istənilən varlıq nəzərdə tutulur (adlanır). Bir çox hallarda obyektlər çoxluğuna əlçatanlıq ilə subyektlər çoxluğuna əlçatanlığın kəsişmədiyini qeyd edirlər. Bəzi hallarda əlçatanlıq subyektinə sistemdə yerinə yetirilən prosesləri aid edirlər. Amma əlçatanlıq subyekti kimi istifadəçinin adını hesab etmək məntiqə uyğundur (o adı ki, proses həyata keçirilir). Əlçatanlıq subyekti kimi kompüterdə işləyən fiziki istifadəçi deyil, əməliyyat sistemində yerinə yetirilən prosesin "məntiqi" istifadəçisinin adı götürülür.

Beləliklə, obyekt əlçatandır - nəyə görə əlçatanlıq yerinə yetirilir, subyekt əlçatandır – kimə görə əlçatanlıq yerinə yetirilir, üsul (metod) əlçatandır – necə əlçatanlıq yerinə yetirilir kimi qəbul olunmalıdır.

Obyekt üçün sahib müəyyən oluna bilər. Sahib – cari obyektin kimə məxsus olduğunu müəyyən edən, obyektdə olan informasiyanın konfidensiallığına cavabdehlik daşıyan, obyektə əlçatlıq və obyektin tamlığına görə məsuliyyət daşıyan subyekt qəbul olunur.

Adətən obyektin sahibi avtomatik olaraq cari obyekti yaradanı subyekt kimi təyin edir, sonrakı mərhələlərdə isə obyektin sahibi obyektə əlçatanlıq üsuluna uyğun olaraq dəyişə bilər. Amma sahib qanuna görə başqa subyektlərin cari obyektə daxil olmalarına konkret məhdudiyyətin qoyulmasına cavabdehlik daşıyır.

Obyektə əlçatanlıq hüquqi (ixtiyarı) obyektə daxil olmaq üçün yerinə yetirilən bir para və ya qrup halında olan üsullar adlanır. Məsələn, əgər istifadəçinin faylı oxumağa imkanı varsa, onda onun bu faylı oxumağa da ixtiyarı

vardır.

Əlçatanlığın məhdudlaşdırılması qanunları.

Fəaliyyətdə olan əməliyyat sistemində qanunlar system administratoru tərəfindən cari təhlükəsizlik siyasətini müəyyən edən zaman müəyyin edilir. Bu qanunlara nəzarət əməliyyat sistemində müdafiənin altsisteminin bir hissəsi olan istinad monitoru tərəfindən yerinə yetirilir.

Əlçatanlığın məhdudlaşdırılması qanunları aşağıdakı tələbləri yerinə yetirməlidir:

1. Əməliyyat sisteminə quraşdırılmış, təşkilat tərəfindən qəbul edilmiş, qanunlara analoji olaraq uyğun olan qanunları dəstəkləməlidir, yəni qoyulmuş qanunlara əsasən istifadəçi qeyriqanuni informasiyaya əlçatanlıq edirsə, onda istifadəçiyə bu əlçatanlıq qadağan olunmalıdır.
2. Əməliyyat sisteminin normal işləməsinə maneçilik edən, qeyriqanuni yerinə yetirilən, dağıdıcı təsir göstərən subyektlərin əməliyyat sisteminə daxil olmasına yol verilməməlidir.
3. Hər bir obyektin sahibi olmalıdır. Heç kimin obyekti olmayan obyektin (sahibsiz obyektin) varlığı icazə verilən deyil.
4. Heç bir subyektin müraciət edə bilməyəcəyi və yaxud, heç bir qanuna riayət edə bilməyən obyektin olmasına icazə verilmir.
5. Məxfi informasiyanın axmasına icazə verilməməlidir.

Əlçatanlığın iki əsas modeli mövcuddur:

1. Seçməklə (diskression);
2. Müvəkkil (mandatlı).

Seçməklə olan modeldə subyekt və ya subyektlər qrupu üzərində konkret əməliyyatın aparılmasına ya icazə verilir,

ya da ki, icazə verilmir. Əksər əməliyyat sistemləri seçməklə üsulundan bəhrələnirlər.

Müvəkkil üsulunda bütün obyektlər məxfilik səviyyəsindədirlər, amma subyektlər isə informasiyaya əlçatanlıq səviyyəsinə uyğun ierarxiya əmələ gətirirlər. Bəzən model təhlükəsizliyin çoxsəviyyəli modeli adlandırılır. Model məxfiliyin saxlanması üçün yararlıdır.

§14. Kompüter virusu anlayışı və növləri

İnformasiyanın qorunması üçün əsas təhlükələrdən biri kompüterə "girmiş" ziyanverici proqramlardır. Belə ziyanverici proqramlar verilənlərin tamlığı üçün də təhlükə yarada bilər. Kompüterdə saxlanılan verilənlərə və proqramlara zərər vuran proqramlara ziyanverici proqramlar deyilir.

Ziyanverici proqramların ən geniş yayılmış növü kompüter viruslarıdır. Kompüter virusu proqramın, sənədin içərisinə, yaxud verilənlər daşıyıcısının müəyyən sahələrinə daxil olan parazit proqram kodudur. Bu kod daxil olduğu kompüterdə özü-özünü çoxalda, müxtəlif ziyanlı işlər görə bilər.

Özü-özünü çoxaltma qabiliyyəti virus proqramlarının başlıca xüsusiyyətidir. Bu proqramlar kompüter və digər daşıyıcıların sahiblərinin xəbəri olmadan öz nüsxələrini yaradır. Virus proqramlarının əksəriyyəti ziyan vurmaqla məşğuldur: verilənləri məhv edir və kompüterin normal

işini pozur.

Kompüter şəbəkələrində bir kompüterə düşmüş ziyanverici proqramın qarşısı vaxtında alınmadıqda, o, nəzarətsiz olaraq həmin kompüterdən digərlərinə yayıla, nəticə etibarı ilə bu problem "həqiqi epidemiya" xarakteri ala bilər.

Bu gün bir çox istifadəçilər bu və ya digər şəkildə kompüterlərdə peyda olan bütün ziyanverici proqramları kompüter virusları adlandırırlar. Əslində bu belə deyil. Belə ki, elə ziyanverici proqramlar var ki, onların reallaşdırılması üçün müxtəlif virus texnologiyalarından istifadə olunmasına baxmayaraq mahiyyət etibarı ilə virus deyillər.

Son dövrlərdə müşahidə olunan tendensiyanın təhlili göstərir ki, hakerlər və digər ziyankarlar ziyanverici proqramların yaradılması və yayılmasından qeyri-leqal gəlir əldə etmək məqsədi güdürlər.

Ehtimal olunur ki, "virus" sözü ilk dəfə 1970-ci ilin mayında Venture jurnalında dərc olunan "Çapıqlı adam" elmi fantastika hekayəsində Qreqori Benford tərəfindən proqrama münasibətdə istifadə edilib.

Kompüter virusları – kompüterdə çoxalmaq, həmçinin rabitə kanalları, kompüter şəbəkələri və informasiya daşıyıcıları (CD və maqnit disklər, flaş qurğuları və s.) vasitəsilə digər kompüterlərə və şəbəkələrə yayılmaq (ötürülmək) qabiliyyətinə malik olan ziyanverici proqramlardır.

Kompüter sisteminə nüfuz edərək virus özünü zərərsiz vizual və ya səs effektləri ilə məhdudlaşdıra bilər, lakin o, həmçinin məlumatların itirilməsinə və ya korlanmasına, şəxsi və məxfi məlumatların sızmasına səbəb ola bilər. Ən

pis halda, virusa yoluxmuş kompüter sistemi işləmir və ya təcavüzkarın tam nəzarəti altında olur.

Virusun müəllifi zərərli təsirləri proqramlaşdırmasa belə, virus səhvlər və əməliyyat sistemi və digər proqramlarla qarşılıqlı əlaqənin hesablanmayan incəlikləri səbəbindən kompüterin çökməsinə səbəb ola bilər. Bundan əlavə, viruslar adətən RAM və ya saxlama cihazlarında müəyyən yer tutur, bəzən kifayət qədər əhəmiyyətlidir və bəzi digər sistem resurslarını götürür.

Buna görə də viruslar zərərli proqram kimi təsnif edilir.

Kompüter viruslarının müəllifləri

Viruslar öz-özünə yaranmır, insanlar tərəfindən yaradılır. Virus müəlliflərini zərərli proqram təminatı yaratmağa və yaymağa məcbur edən ən çox ehtimal olunan səbəblər bunlardır:

- adi gənclik xuliqanlığı , əldə edilmiş intellektual səviyyə əsasında özünü təsdiq etmək cəhdləri. Əslində, bu cür kompüter xuliqanlığı adi küçə xuliqanlığından heç bir fərqi yoxdur, yalnız "özünü təsdiqləmə" ya xiyabanda, ya da onlayn rejimdə baş verir;

- qurbanın resurslarını mənimsəmək məqsədi ilə fırıldaqçılıq, kompüterə gizli nəzarət, İnternetə giriş parollarının, WebMoney "pul kisələrindən" pul vəsaitlərinin və şəxsi bank hesablarına giriş kodlarının oğurlanması (əgər qurban bu xidmətdən istifadə edirsə).

Əgər korporativ şəbəkələrə hücum edilirsə, o zaman söhbət casusluqdan gedir: bir qayda olaraq, bu, maliyyə dəyəri olan məxfi məlumatların mənimsənilməsi məqsədi ilə şəbəkəyə daxil olmaqdır.

Virusların əsas hissəsini proqramlaşdırma dilini yenicə öyrənmiş və bu dildə güclərini sınamaq istəyən tələbələr və

məktəblilər yaradır. Belə virusların əhəmiyyətli bir hissəsi çox vaxt onların müəllifləri tərəfindən yayılmır.

İkinci qrup da özlərini virus yazmağa və yaymağa həsr etməyə qərar verən gənclərdən (adətən tələbələr) ibarətdir. Bir qayda olaraq, onlar "klassik" virusların və ya son dərəcə primitiv olan və çoxlu sayda səhvləri olan virusların çoxsaylı modifikasiyalarını yaradırlar. Onlar tez-tez virus konstruktorlarından istifadə edirlər, onların köməyi ilə hətta əməliyyat sistemi haqqında minimal biliklərlə belə yeni viruslar yarada bilirlər.

Yaşlandıqca və daha təcrübəli olduqda, bu virus yazıçılarının çoxu "peşəkar" viruslar yaradan və dünyaya buraxan üçüncü, ən təhlükəli qrupa düşür. Bunlar diqqətlə düşünülmüş və düzəldilmiş proqramlardır.

Virus müəlliflərinin dördüncü qrupu "tədqiqatçılardır". Bu qrup yoluxma, gizlətmə, antiviruslara qarşı mübarizə və s. əsaslı şəkildə yeni üsullar icad etməklə məşğul olan istedadlı proqramçılardan ibarətdir. Bu proqramçılar virusları özləri üçün deyil, daha çox "kompüter virusologiyasının" potensialını "kəşf etmək" naminə yazırlar.

Kompüter viruslarının tarixi

Bu gün kompüter virusunun otuz ildən çox yaşı var.

İlk məlum viruslar 1981-ci ildə ortaya çıxan Apple II PC üçün Virus 1,2,3 və ElkClonerdir. İlk virus epidemiyaları 1987-1989-cu illərə təsadüf edir. Brain (McAfee Jerusalem- ə görə 18 mindən çox yoluxmuş kompüter vbirusa yoluxmuşdur), Morris qurdu (6200-dən çox kompüter, əksər şəbəkələr beş günə qədər sıradan çıxdı), DATACRIME (təkcə Hollandiyada təxminən 100 min yoluxmuş kompüter).

1990-cı ildə ilk kommersiya antivirusu Symantec NortonAntiVirus çıxdı.

Sonrakı bir neçə il ərzində sistemə daxil olmaq və faylları yoluxdurmaq üçün ən qeyri-adi üsullar sınaqdan keçirildi (Direktor II - 1991, PMBS, Shadowgard , Cruncher - 1993). Bundan əlavə, obyekt fayllarını (Shifter , 1994) və proqramın mənbə kodlarını (SrcVir, 1994) yoluxduran viruslar meydana çıxdı . Microsoft Office paketinin yayılması ilə makro viruslar geniş yayıldı (Concept , 1995).

Şəbəkələrin və İnternetin yayılması ilə fayl virusları getdikcə əsas iş kanalı kimi onlara diqqət yetirir (Melissa , 1999 - yayılma sürətinə görə bütün rekordları qıran makro virus və şəbəkə qurdu).

MsBlast (Microsoft-a görə - 16 milyondan çox sistem), Sasser və Mydoom (müvafiq olaraq 500 milyon və 4 milyard dollar təxmin edilən zərər) istismar qurdları tərəfindən törədilib.

Bundan əlavə, monolit viruslar öz yerini rolların və köməkçi alətlərin ayrılması ilə mürəkkəb zərərli proqramlara verir. Sosial texnologiyalar - spam və fişinq proqram təminatının təhlükəsizlik mexanizmlərindən yan keçmək üçün yoluxma vasitəsi kimi də inkişaf edir.

Virusların ən müasir növü - soxulcan- botnetlər getdikcə sürət qazanır (Rustok , 2006, təxminən 150 min bot; Conficker , 2008-2009, 7 milyondan çox bot; Kraken, 2009, təxminən 500 min bot).

Viruslar, digər zərərli proqramlar arasında, nəhayət kibercinayətkarlıq vasitəsi kimi rəsmiləşdirilir.

Kompüter viruslarının yayılması üsulları

Kompüter viruslarının yayılma yolları müxtəlifdir, lakin

hələ də əsas ehtiyat tədbirlərinə əməl etməklə özünüzü qoruya biləcəyiniz ən çox yayılmış viruslar var.

- **Floppy disklər.** 1980-1990-cı illərdə ən çox yayılmış infeksiya kanalı. İndi daha çox yayılmış və səmərəli kanalların ortaya çıxması və bir çox müasir kompüterlərdə disket sürücülərinin olmaması səbəbindən praktiki olaraq yoxdur
- **Fleş disklər (flash disklər).** Hazırda USB fleş disklər disketləri əvəz edir və onların taleyini təkrarlayır - çoxlu sayda viruslar çıxarıla bilən yaddaş qurğuları, o cümlədən rəqəmsal kameralar, rəqəmsal video kameralar, portativ rəqəmsal pleyerlər vasitəsilə yayılır və 2000-ci illərdən etibarən mobil telefonlar, xüsusən də smartfonlar getdikcə daha mühüm rol oynadı.
- **E-poçt.** Tipik olaraq, e-poçtlardakı viruslar zərərsiz əlavələr kimi maskalanır: şəkillər, sənədlər, musiqi, veb-saytlara keçidlər. Bəzi e-poçtlarda əslində yalnız linklər ola bilər, yəni e-poçtların özündə zərərli kod olmaya bilər, lakin belə bir keçidi açsanız, virus kodu olan xüsusi yaradılmış vebsayta daxil ola bilərsiniz.
- **Ani mesajlaşma sistemləri.** ICQ və digər ani mesajlaşma proqramları vasitəsilə guya fotoşəkillərə, musiqilərə və ya əslində virus olan proqramlara keçidlər göndərmək də adi haldır.
- **Veb səhifələr.** İnternet səhifələri vasitəsilə yoluxma həm də Ümumdünya İnternet səhifələrində müxtəlif "aktiv" məzmunun olması səbəbindən mümkündür (skriptlər, ActiveX komponentləri).

Kompüter viruslarının yayılmasının bir çox yolu var. İnfeksiyanın qarşısını almaq üçün əsas ehtiyat tədbirləri görməlisiniz:

- İnternetdə yalnız etibarlı mənbələrdən istifadə etməyə çalışın;
- şübhəli proqramları yükləməyin və şübhəli şəkillərə klikləməyin;
- Naməlum alıcıdan məktublar alarkən, əlavə edilmiş faylların uzadılmasına diqqət yetirin. Əgər onların: *.bat, *.vbs, *.scr, *.exe kimi növləri varsa, onda siz bu proqramları yükləməməlisiniz, onlar yoluxmuş ola bilər və ya sadəcə olaraq Trojan virusu ola bilər;
- lisenziyalı antiviruslardan istifadə edin.

Bu halda asanlıqla kompüterin virusa yoluxmasından qaça bilərsiniz.

Virusa yoluxmanın əlamətləri

Kompüter bir virusa yoluxduqda, onu aşkar etmək üçün onun əsas əlamətlərini bilməlisiniz:

- əməliyyatın dayandırılması və ya əvvəllər uğurla işləyən proqramların düzgün işləməməsi;
- kompüterin yavaş işləməsi;
- əməliyyat sistemini yükləmək mümkün olmaması;
- faylların və kataloqların yoxa çıxması və ya onların məzmununun təhrif edilməsi;
- faylın dəyişdirilməsi tarixinin və vaxtının dəyişdirilməsi;
- fayl ölçüsünün dəyişdirilməsi;
- diskdəki faylların sayında gözlənilməz əhəmiyyətli artım;
- pulsuz RAM ölçüsünün əhəmiyyətli dərəcədə azalması;
- gözlənilməz mesajların və ya şəkillərin ekranda göstərilməsi;

- gözlənilməz səs siqnallarının verilməsi;
- Kompüterdə tez-tez donmalar və qəzalar.

Qeyd etmək lazımdır ki, yuxarıda göstərilən hadisələr mütləq virusun olması ilə bağlı deyil, digər səbəblərin nəticəsi ola bilər. Buna görə də, kompüterin vəziyyətini düzgün diaqnoz etmək həmişə çətindir.

Yalnız müəyyən hallarda kompüter virusuna yoluxa bilərsiniz:

- kompüterdə virusla yoluxmuş icra olunan proqramın işə salınması;
- yükləmə virusu olan diskdən (disketdən) kompüterin yüklənməsi;
- yoluxmuş sürücünün sistemə qoşulması;
- makro virusla yoluxmuş sənədin açılması;
- yoluxmuş əməliyyat sisteminin kompüterə quraşdırılması.

Qeyd etmək lazımdır ki, əksər hallarda məhz serverlər kompüter viruslarının hədəfinə çevrilir. Bir qayda olaraq, kompüter şəbəkələri, o cümlədən İnternet virusların yayılması üçün potensial vasitə rolunu oynayır. Belə ki, virusların serverdə olan proqramlara yoluxması, şəbəkə vasitəsilə ona qoşulmuş kompüterlərə (işçi stansiyalara) yayılması və bütün şəbəkəyə ciddi ziyan vura bilməsi ehtimalı daha böyükdür.

Bəzən kompüter virusu yarandığı ilk anda fəaliyyət göstərmir. Kompüterin yaddaşında və ya proqramlarda "yaşayan" belə viruslar yalnız müəyyən olunmuş vaxtlarda işə düşür. Viruslar emal olunan bütün informasiyaları izləyir, informasiya bir yerdən başqa yerə ötürüldükdə virus da onunla birlikdə yerini dəyişir.

İnformasiya təhlükəsizliyi baxımından kompüter

viruslarının müsbət cəhətini də qeyd etmək lazımdır. Belə ki, proqram təminatlarında virusların mövcud ola bilməsi faktı proqram oğurluğunun qarşısının alınmasında yaxşı mühafizəçi rolunu oynayır.

Bəzən proqramı hazırlayanlar öz proqramlarını və disklərini hər hansı virusla qəsdən yoluxdururlar ki, icazəsiz şəkildə proqramı və ya diski köçürənlər kompüterlərində virusların yayılması problemi ilə qarşılaşsınlar.

Troyan proqramları

Troyan proqramları (və ya troyan atları) – yad kompüterlərə uzaq məsafədən girişi təqdim edən, həmin kompüterdə müxtəlif manipulyasiyalar etməyə, məxfi məlumatları (parolları, kredit kartların nömrələrini, İnternetə və kompüterə giriş adlarını və s.) ötürməyə imkan verən ziyanverici proqramlardır. Onlar kompüter virusları deyillər, hər hansı pozucu funksiyaya malik olmur və digər kompüterlərin idarə olunması və ya orada yerinə yetirilən proseslərin nəzarət edilməsi üçün nəzərdə tutulmuşdur.

Troyan proqramları, adətən, başqa faylları yoluxdurmur, öz-özünə çoxalmırlar, amma məşhur (geniş yayılmış) proqramlarda maskalanaraq istifadəçini həmin proqramı öz kompüterinə köçürməyə və ziyanvericini kompüterdə quraşdıraraq işə salmağa təhrik edirlər.

Kompüterə düşdükdən sonra troyan proqramları özünü şübhə doğurmayan (məsələn, winrun32dll.exe) adla sistem qovluqlarına köçürür. Bundan sonra əməliyyat sistemi yenidən yüklənəndə yerinə yetirilən proqramların qeydiyyatının aparıldığı reyestrə (HKEY_LOCAL_ MACHINE\-SOFTWARE\Microsoft\Windows\ CurrentVersion\Run), eləcə də Run, RunOnce, Runservices, RunservicesOnce

adlı bölmələrə yazır.

Yerinə yetirdiyi ziyanverici hərəkətlərinə görə troyan proqramlarını şərti olaraq aşağıdakı növlərə bölmək olar:

- uzaq məsafədən icazəsiz idarəetmə utilitləri– yoluxmuş kompüterin bədniyyətli şəxs tərəfindən uzaq məsafədən idarə edilməsinə imkan verir;
- DDoS (Distributed Denial of Service – "xidmət göstərməkdən imtina edilməsi") həyata keçirmək üçün utilitlər–yoluxmuş kompüterin informasiya sisteminin resurslarını tükəndirir ki, bunun da nəticəsində sistem öz funksiyalarını yerinə yetirə bilmir və əlçatmaz olur;
- casus proqramları-istifadəçinin hərəkətlərini gizli olaraq müşahidə edir və bədniyyətli şəxsi maraqlandıran məlumatları öz "jurnalına" yazır;
- reklam proqramları – daha tez-tez istifadə olunan proqramlara reklam və elan xarakterli məlumatları yerləşdirməyə imkan verir;
- zəngetmə proqramları – modem və ya telefon xətlərinin köməyi ilə kommersiya əsaslı serverə zəng edərək istifadəçini xidmətlərin haqqını ödəməyə təhrik edir;
- spamların yayılması serveri – kənar şəxsin kompüterini spamların yayılması serverinə çevirməyə imkan verir;
- çoxkomponentli troyan proqramları-yükləyicilər digər ziyanverici proqramları və ya onların komponentlərini İnternetdən köçürür və sistemə yeridir.

Troyan viruslarının müasir dövrdə daha tez-tez istifadə olunan əsas aşağıdakı növlərini qeyd etmək olar:

Mail Senders, BackDoor, Log Writers или KeyLoger.

Mail Senders – quraşdırıldığı kompüterdən məlumatları "sahibinə" göndərir. Bu tip troyan viruslarını digər kompüterlərə yeridən şəxslər onların köməyi ilə İnternetə, o cümlədən ICQ, elektron poçtu, Chat xidmətlərinə giriş parollarını əldə edə bilər. Bu zaman hətta kompüter sahibinin xəbəri olmur ki, kimsə onun poçtunu oxuyur, onun adından İnternetə qoşulur, ICQ identifikatorundan istifadə etməklə əlaqə siyahısında olan digər istifadəçilərə analoji troyan viruslarını yayır. MailSender sahibindən, yəni onu quraşdıran şəxsdən asılı olmadan fəaliyyət göstərir, ona bütün "tapşırıqlar" quraşdırılma zamanı verilir və o, bütün funksiyalarını plan üzrə həyata keçirir.

BackDoor – Mail Sender troyan viruslarının bütün imkanlarını yerinə yetirməklə yanaşı digər kompüterlərin uzaq məsafədən (məsələn İnternet vasitəsilə) idarə edilməsi üçün 10-a qədər əlavə funksiya təqdim edir. BackDoor sözünün hərfi tərcüməsi arxa qapı və ya gizli giriş məna- sını verir.

Belə troyan virusları istənilən şəxsə yoluxmuş kompüterə tam giriş imkanı verir. O, müştərinin qoşulmasını gözləyir. Yoluxmuş kompüterdə müştəri İnternetə və ya lokal şəbəkəyə qoşulduqdan sonra troyan virusu topladığı məlumatları öz sahibinə göndərir və bu kompüterə girişi açır. Belə ki, o, müəyyən sistemdə şəbəkə portlarını açır və bu barədə öz sahibinə məlumat verir.

BackDoor proqramları iki növə bölünürlər:

Lokal BackDoor – müəyyən lokal imtiyazlar təqdim edir. Məsələn, kompüterdə qeydiyyatdan keçmiş bir neçə istifadəçi sistem inzibatçısının hüquqlarına malik olmurlar, lakin kompüterə yeridilmiş lokal BackDoor troyan virusu onun sahibi olan istifadəçiyə sistem inzibatçısının

hüquqlarını təqdim edir.

Uzaqda olan BackDoor – uzaq məsafədən kompüterə shell təqdim edə bilər. Girişin təqdim edilməsi – shell proqramının iki növü mövcuddur: BindShell və Back Connect.

BindShell – daha geniş yayılmışdır, "müştəri-server" texnologiyasına əsasən işləyir, yəni sahibinin qoşulmasını gözləyir.

Back Connect – brandmauerləri adlamaq üçün tətbiq olunur. O, sahibinin kompüterinə qoşulmağa cəhd edir.

Log Writers və ya Key loggers – kompüterdə klaviaturadan daxil edilən bütün məlumatları köçürür və fayla yazır. Bu fayl sonradan ya elektron poçtu vasitəsilə müəyyən ünvana göndərilir, ya da FTP vasitəsilə baxılır.

Son vaxtlar bu proqramlar bir sıra əlavə funksiyalar da yerinə yetirirlər:

- proqramların pəncərələrindən informasiyanın tutulması;
- siçanın düyməsinin basılmasının tutulması;
- ekranın və aktiv pəncərələrin şəklinin çəkilməsi, göndərilən və alınan bütün məktubların qeydiyyatının aparılması;
- faylların istifadəsi fəallığının, sistem reyestrinin və printerə göndərilmiş tapşırıqlar növbəsinin monitorinqi, kompüterə qoşulmuş mikrofondan səsin və veb-kameradan videonun tutulması və s.

Key loggers proqramlarının beş növü məlumdur:

- hökumət təşkilatlarının himayəsi altında işlənib hazırlanan və tətbiq edilən (məsələn, ABŞ-da Magic Lantern proqramı, Cyber Knight layihəsi) casus proqramları;

- müxtəlif əməliyyat sistemlərinin istehsalçıları tərəfindən işlənib hazırlanan və əməliyyat sisteminin özəyinə daxil edilən casus proqramları;
- istifadəçinin kompüterindən mühüm informasiyanın oğurlanması ilə bağlı konkret məsələnin həlli üçünməhdud sayda (çox vaxt bir və ya bir neçə nüsxədə) yaradılan casus proqramları;
- kommersiya, xüsusən, korporativ proqramlar – çox nadir hallarda siqnatura bazasına daxil edilirlər (yalnız siyasi motivlərə görə daxil edilə bilər);
- virus proqramlarının tərkibinə daxil olan keylogging modulundan ibarət olan casus proqramları. Siqnatura məlumatları virus bazalarına daxil edilənədək bu modular naməlum qalırlar. Belə proqramlara nümunə kimi klaviaturada düymənin basılmasının tutulması və əldə olunmuş məlumatların İnternet vasitəsilə ötürülməsi modulunu özündə saxlayan məşhur virusları göstərmək olar.

Bundan əlavə, troyan proqramlarının daha iki növü mövcuddur:

1. Trojan-Dropper
2. Trojan-Downloader.

Hər iki proqramın məqsədi kompüterə şəbəkə qurdu və ya troyan atı kimi ziyanverici proqramların yüklənməsindən ibarətdir, yalnız onların fəaliyyət prinsipləri fərqlənir.

Trojan-Dropper özündə artıq məlum ziyanverici proqramları saxlaya və ya onların yeni versiyalarını yük- ləyə bilər. Onlar kompüterə bir deyil, eyni zamanda bir- birindən fərqlənən və ayrı-ayrı adamlar tərəfindən yazılmış bir neçə ziyanverici proqramı yükləyə

bilər.

Trojan-Downloader proqramları virus yazanlar tərəfin- dən fəal istifadə olunur. Bunun əsas səbəbləri məlum troyan proqramlarının onun tərkibində gizlədilməsinin mümkün- lüyü, onun ölçüsünün *Trojan-Dropper* proqramlarına nis- bətən kiçik olması, eləcə də troyan viruslarının yeni versiya- larının işə salınmasının asanlığı ilə bağlıdır.

Hər iki növ ziyanverici proqramlar yalnız troyan proqramlarının deyil, həmçinin müxtəlif virus, reklam (adware) və ya pornoqrafik (pornware) proqramların kompüterlərdə quraşdırılması üçün istifadə olunur.

Spamlar

Spam – xüsusi proqramlar vasitəsilə siyasi, kommersiya, reklam və digər növ məlumatların, bu məlumatları almaq arzusunu bildirməyən insanlara kütləvi və anonim şəkildə göndərilməsidir.

Burada *anonim yayma* dedikdə məlumatların gizli və ya saxta əks ünvanla avtomatik yayılması başa düşülür. Hazırda elə spam göndərən yoxdur ki, o öz ünvanını və göndərmə yerini gizlətməsin.

Kütləvi yayma hər hansı spam göndərən tərəfindən müəyyən məlumatın eyni zamanda yüzlərlə, minlərlə, hətta milyonlarla ünvana göndərilməsini nəzərdə tutur.

Qeyd etmək lazımdır ki, məktubun səhvən başqa ünvana göndərilməsi spam deyil, arzuolunmaz poçt kimi qəbul edilir. *Alınması arzu olunmayan göndərişi* alan şəxsin arzusunun, hətta iradəsinin əksinə olaraq hər hansı məlumatın onun ünvanına göndərilməsini ehtiva edir. Lakin konfranslar və planlaşdırılan digər tədbirlər barədə məlumatlandırıcı poçt göndərişləri spamlara aid

edilməməlidir.

Spamların daha geniş yayılmış növlərinə aşağıdakılar aid etmək olar:

- *Reklam*. Leqal bizneslə məşğul olan bəzi şirkətlər öz məhsullarını və xidmətlərini daha ücüz və rahat yolla spamların köməyi ilə yayırlar. Onlar öz reklam- larının yayılmasını müstəqil şəkildə özləri həyat keçirə və ya bu sahədə ixtisaslaşan təşkilatlara (şəxslərə) sifariş edə bilərlər.
- *Qeyri-qanuni məhsulun reklamı*. Spamlar vasitəsilə çox vaxt başqalarına məlumat vermək, yaymaq mümkün olmayan məhsulları (pornoqrafiyanı, saxta malları, dövriyyəsi məhdudlaşdırılmış dərman məh- sullarını, qeyri-qanuni yolla alınmış gizli məlumat- ları, verilənlər bazasını və s.) reklam edirlər.
- *Əks-reklam*. Spam, həmçinin, reklam haqqında qa- nunla qadağan edilmiş (məsələn, rəqibləri və onları pisləyən, ləkələyən) informasiyanın yayılması üçün istifadə olunur.
- *Nigeriya məktubu*. Spam məktub göndərilən adamdan pul qoparmaq üçün istifadə olunur. Belə məktublar daha çox Nigeriyadan göndərildiyinə görə onları daha çox "Nigeriya məktubları" adlandırırlar. Belə məktublarda məlumat verilir ki, məktubu alan şəxs hər hansı yolla böyük məbləğdə pul əldə edə bilər və məktub göndərən bu işdə ona kömək edə bilər. Maraq göstərildiyi halda, məktub göndərən müxtəlif bəhanələrlə (bankda hesab açmaq, sənədləri rəsmiləşdirmək və s.) bir az pul köçürülməsini xahiş edir. Fırıldaqçıların məqsədi məhz bundan ibarətdir. Belə fırıldaqçılığın nisbətən az yayılmış adı *skam* və ya

skam419 (Nigeriya CM-də maddənin nömrəsinə uyğun olaraq) adlanır.

- *Fişinq*. İngilis dilində olan "phishing" və ya "fishing" (balıq tutmaq) sözündəndir. Məktub göndərən alan şəxsdən kredit kartının nömrəsinivə ya elektron (online) ödəmə sisteminə giriş parolunu öyrənmək üçün fişinq texnologiyasından istifadə edir. Belə məktublar, adətən, bankın inzibatçıları tərəfindən yazılmış məktub kimi göndərilir. Məsələn, məktubda göstərilir ki, müştəri özü haqqında məlumatları təsdiq etməlidir, əks halda onun hesabı bağlanacaqdır. Sonda ona doldurmaq üçün müvafiq formanın yerləşdiyi saytın ünvanı təklif olunur. Bu formada digər məlumatlarla yanaşı lazım olan rekvizitlərin də doldurulması tələb olunur.

Praktikada spamların aşağıdakı növlərindən də istifadə olunur:

- xoşməramlı məktublar;
- siyasi təbliğatın yayılması;
- poçt sisteminin sıradan çıxarılması üçün kütləvi göndərişlər təşkil etmək;
- hər hansı şəxsə qarşı mənfi münasibət yaratmaq məqsədilə onun adından kütləvi göndərişlər təşkil etmək;
- kompüter viruslarını saxlayan məktubların kütləvi göndərilməsini təşkil etmək.

Qeyd etmək lazımdır ki, müəyyən növ məlumatların kütləvi yayılması üçün alanların razılığının tələb olunmaması azadlığı (qanuniliyi) hər bir ölkənin qanun-vericiliyində təsbit oluna bilər. Məsələn, yaxınlaşan təbii fəlakət, vətəndaşların kütləvi səfərbərliyi, seçkilər və s.

barədə məlumatlar üçün yayılma azadlığı təmin edilə bilər.

Lakin insanların almaq istəmədiyi məlumatların onların iradəsinin əleyhinə göndərilməsi arzuolunmaz haldır. Bu, insanların vaxtının və maddi imkanlarının lazımsız sərfinə, mənəvi və fiziki yüklənməsinə səbəb olur. Belə məlumatlar son dövrlərdə elektron informasiya vasitələri (İnternet, mobil telefonlar, televiziya və radio və s.) ilə daha çox yayılmağa başlanmışdır.

Spamlar yayılması aşağıdakı yollarla həyata keçirilə bilər:

- Elektron poçtu. Spamların yayılması üçün müəyyən zəif yerləri olan və ya imkanlar yaradan serverlərdən, veb-mail serverlərindən, kompüter zombilərdən və s. istifadə olunur.
- Usenet. Hazırda istifadəçilər əksər, ələlxüsus nizamlanmayan Usenet xəbərlər qruplarını tərk edir və nizamlanan konfranslardan istifadə edirlər, çünki ənənəvi Usenet qrupları, demək olar ki, yalnız reklamları özündə saxlayır.
- Məlumatların ani göndərilməsi, yəni interaktiv məlumat mübadiləsini təmin edən sistemləri (ICQ və s.) də spamların göndərilməsi üçün fəal istifadə olunur. Belə spamları SPİM (SPam + Instant Messenger) adlandırırlar.
- SPIT (Spam over IT) – IP-telefon vasitəsilə yayılan spam.
- Bloqlar, vikilər, forumlar və elan lövhələri. Son dövrlərdə istifadəçilərə öz qeydlərini yazmaq, məlumatlar daxil etmək, dəyişikliklər aparmaq və s. imkanları verən veb-saytlar geniş yayılmışdır. Məhz bu imkanlardan spamların göndərilməsi və yayılması

üçün istifadə edirlər.

- Şəbəkə məlumatları, o cümlədən şəbəkə ilə reklam məlumatlarının göndərilməsi.
- SMS-məlumatlar. Mobil telefonlara spam xarakterli SMS-mesajların göndərilməsi üçün geniş istifadə olunur.

Şəbəkə qurdları

Şəbəkə qurdları kateqoriyasına ziyanvericilik fəaliyyətini həyata keçirmək məqsədilə öz sürətlərini aşağıdakı yollarla lokal və ya qlobal kompüter şəbəkələri vasitəsilə yayan ziyanverici proqramlar aid edilir:

- uzaq məsafədə olan kompüterlərə soxulmaq;
- öz surətini uzaq məsafədə olan kompüterlərdə işə salmaq;
- gələcəkdə şəbəkənin digər kompüterlərinə yayılmaq.

Şəbəkə qurdları disklərdə olan faylları dəyişdirmirlər, lakin kompüter şəbəkələrində yayılır, kompüterin əməliyyat sisteminə girir, digər kompüterlərin və ya istifadəçilərin ünvanlarını tapır və müxtəlif yayılma vasitələrindən istifadə etməklə özünün surətlərini həmin ünvanlara göndərir.

Özlərinin yayılması üçün şəbəkə qurdları müxtəlif kompüter və mobil şəbəkələrdən istifadə edirlər. Belə şəbəkələrə misal olaraq aşağıdakıları göstərmək olar:

- İnternet, o cümlədən elektron poçtu;
- məlumatların ani (interaktiv) mübadiləsi sistemləri;
- faylların mübadiləsi şəbəkələri;
- lokal şəbəkələr;
- mobil qurğular (telefonlar, cib kompüterləri və s.) arasında məlumatların mübadiləsi şəbəkələri.

Şəbəkə qurdları istifadəçi tərəfindən hər hansı hərəkət

edilmədən yoluxmuş maşınlara daxil olurlar. Onlar öz təbiətlərinə görə bioloji prototiplərinə çox yaxındırlar. Hələ ki, qabaqlayıcı tədbirlər, o cümlədən antivirus skanerləri və vaksinləri şəbəkə qurdları ilə mübarizədə çox qeyri-effektiv olaraq qalırlar. Onlar viruslardan fərqli olaraq, özlərinin yayılması üçün lokal və qlobal şəbəkələrin protokollarından və imkanlarından fəal surətdə istifadə edirlər, ona görə də onları şəbəkə qurdları adlandırırlar.

Uzaq məsafədə olan kompüterə daxil olmaq və öz surətini işə salmaq üçün şəbəkə qurdları müxtəlif üsullardan istifadə edirlər:

- sosial mühəndislik – social engineering (məsələn, qoşma faylı açmağa çağıran elektron məktubun mətni);
- şəbəkənin konfiqurasiyasında olan nöqsanlar (məsələn, tam giriş üçün açıq olan diskə köçürmə);
- əməliyyat sistemlərinin və əlavələrin təhlükəsizlik xidmətlərində səhvlər;
- xüsusi toplayıcı proqram – virus və ya qurd olmayan
- bu proqram özü kompüterə daxil olur, sonra isə şəbəkə qurdunu və ya virusu hissə-hissə şəbəkədən kompüterə köçürür. Qurd və ya virus kompüterə hissə-hissə köçürüldüyündən antivirus proqramları onu aş- kar edə bilmir.

Bəzi şəbəkə qurdları digər ziyanverici proqramların xassələrinə malik olurlar. Məsələn, bəzi şəbəkə qurdları özündə troyan funksiyalarını saxlayır və ya kompüter viruslarına analoji olaraq lokal diskdə yerinə yetirilən faylları yoluxdura bilirlər. Başqa sözlə, şəbəkə qurdları troyan proqramlarının və ya kompüter viruslarının xassələrinə malik olurlar.

Digər ziyanverici proqramlar

Qeyd etmək lazımdır ki, ziyanverici proqramların kifayət qədər müxtəlif növləri mövcuddur. Yuxarıda sadalanan növlərlə yanaşı aşağıdakı ziyanverici proqramların – haker utilitlərinin adlarını da qeyd etmək olar:

RootKit, snifferlər, Exploit, HackTool, Nuker, Flooder, Constructor, Bad-Joke, Hoax, FileCryptor, PolyCryptor, PolyEngine, VirTool, Riskware, Adware (Advware, Spyware, Browser Hijackers), Pornware (Porn-Dialer, Porn- Downloader, Porn-Tool).

İnformasiyanın ziynverici proqramlardan qorunması

Ziyanverici proqramların kompüter sisteminə və ya şəbəkəsinə daxil olması və yayılması, eləcə də onun sahiblərinə maddi və mənəvi ziyan vura bilməsi təhlükələrinin ciddiliyini nəzərə alaraq, KSŞ-nin, eləcə də informasiya resurslarının ziyanverici proqramların hücumundan qorunması üçün daim zəruri tədbirlərin görülməsi, xüsusi proqram təminatlarının (o cümlədən antivirus proqramlarının) işlənib hazırlanması, tətbiq olunması və nəzarətdə saxlanması zəruridir. Bu problem istifadəçilər və şəbəkə

§15. Antivirus proqramları

Viruslarla mübarizədə əsas silah antivirus proqramlarıdır. Onlar yalnız virusları aşkarlamağa deyil, həm də onları kompüterinizdən silməyə imkan verir.

Müasir antivirus texnologiyaları şübhəli faylın kodunu antivirus verilənlər bazasında saxlanılan nümunələrlə müqayisə edərək, demək olar ki, bütün məlum virus proqramlarını müəyyən etməyə imkan verir.

Bundan əlavə, yeni yaradılmış virus proqramlarını aşkar etməyə imkan verən davranış modelləşdirmə texnologiyaları hazırlanmışdır. Aşkar edilmiş obyektlər müalicə edilə, təcrid oluna (karantinə) və ya silinə bilər. Virusdan qorunma iş stansiyalarında, fayl və poçt serverlərində, demək olar ki, hər hansı bir ümumi əməliyyat sistemində işləyən firewalllarda, müxtəlif növ prosessorlarda quraşdırıla bilər.

Virusla yoluxmuş faylların və disklərin vaxtında aşkarlanması və aşkar edilmiş virusların hər bir kompüterdə tam məhv edilməsi virus epidemiyasının digər kompüterlərə yayılmasının qarşısını alır.

Antivirus proqramlarının növləri

Antivirus proqramları tərəfindən istifadə olunan virusların axtarışının bir neçə fundamental metodları vardır. Kompüter viruslarını aşkar etmək, silmək və onlardan qorumaq üçün bir neçə növ antivirus proqramları hazırlanmışdır:

1. detektor proqramları
2. faqlar
3. auditor proqramları (müfəttişlər)
4. filtr proqramları (monitorlar)

5. peyvənd və ya immunizator proqramları
6. skaner

Detektor proqramları

Detektor proqramları operativ yaddaşda və fayllarda müəyyən virusun imza xarakteristikasını axtarır və aşkar edildikdə müvafiq mesaj verir. Belə antivirus proqramlarının dezavantajı odur ki, onlar yalnız belə proqramların tərtibatçılarına məlum olan virusları tapa bilirlər.

Faqlar

Faq proqramları, həmçinin peyvənd proqramları yalnız viruslara yoluxmuş faylları tapmır, həm də onları "müalicə edir", yəni virus proqramının gövdəsini fayldan çıxararaq faylları orijinal vəziyyətinə qaytarır. İşlərinin əvvəlində faqlar RAM-da virusları axtarır, onları məhv edir və yalnız bundan sonra faylları "təmizləməyə" davam edir. Faglar arasında polifaglar, yəni çoxlu sayda virusları axtarmaq və məhv etmək üçün nəzərdə tutulmuş həkim proqramları var.

Auditor proqramları (müfəttişlər)

Auditor proqramları (müfəttişlər) viruslardan ən etibarlı qorunma vasitələrindəndir. Auditorlar (müfəttişlər) diskdəki məlumatları görünməz viruslar üçün yoxlayır, virusun fayllara daxil olub-olmamasını, sabit diskin açılış sektorunda kənar şəxslərin olub olmadığını və ya Windows reyestrində icazəsiz dəyişikliklərin olub olmadığını öyrənirlər. Üstəlik, müfəttiş disklərə daxil olmaq üçün əməliyyat sistemi alətlərindən istifadə edə bilməz (bu o deməkdir ki, aktiv virus bu girişi ələ keçirə bilməyəcək).

Proqramlar - filtrlər (monitorlar)

Filtr proqramları (monitorlar) və ya “gözətçilər” viruslar üçün xarakterik olan kompüter əməliyyatı zamanı

şübhəli hərəkətləri aşkar etmək üçün nəzərdə tutulmuş kiçik rezident proqramlardır. Belə hərəkətlər aşağıdakılardır:

1. COM , EXE uzantıları olan faylları düzəltməyə cəhdlər
2. fayl atributlarını dəyişdirin
3. mütləq ünvanda diskə birbaşa yazmaq
4. diskin yükləmə sektorlarına yazmaq
5. Rezident proqramının yüklənməsi.

Peyvəndlər və ya immunizatorlar

Peyvəndlər və ya immunizatorlar faylların yoluxmasının qarşısını alan rezident proqramlardır. Bu virusu "müalicə edən" həkim proqramları olmadıqda peyvəndlər istifadə olunur. Peyvənd yalnız məlum viruslara qarşı mümkündür. Peyvənd proqramı və ya diski onun işinə təsir etməyəcək şəkildə dəyişdirir və virus onu yoluxmuş kimi qəbul edəcək və buna görə də kök almayacaq. Hazırda peyvənd proqramlarının istifadəsi məhduddur.

Skaner

Antivirus skanerlərinin iş prinsipi faylların, sektorların və sistem yaddaşının yoxlanılmasına, habelə onlarda məlum və yeni (skanerə məlum olmayan) virusların axtarışına əsaslanır. Məlum virusları axtarmaq üçün "maskalar" adlanan vasitələrdən istifadə olunur. Virus maskası müəyyən bir virusa xas olan sabit kod ardıcıllığıdır. Əgər virusun tərkibində qalıcı maska yoxdursa və ya bu maskanın uzunluğu kifayət qədər uzun deyilsə, o zaman başqa üsullardan istifadə edilir.

Bu gün bir çox antivirus proqramları mövcuddur, lakin onların ən son inkişafların öhdəsindən gələ biləcəyinə zəmanət yoxdur. Buna görə bəzi ehtiyat tədbirləri

görülməlidir, xüsusən:

1. Çox zərurət olmadıqca imtiyazlı hesablar altında işləməyin.
2. Şübhəli mənbələrdən tanış olmayan proqramları işlətməyin.
3. Sistem fayllarına icazəsiz dəyişikliklərin mümkünlüyünü əngəlləməyə çalışın.
4. Potensial təhlükəli sistem funksiyalarını söndürün (məsələn, MS Windows-da autorun media, gizlədilmiş faylları, onların uzantılarını və s.).
5. Şübhəli saytlara getməyin, brauzerin ünvan çubuğundakı ünvana diqqət yetirin.
6. Yalnız etibarlı paylamalardan istifadə edin.
7. Daim vacib məlumatların ehtiyat nüsxələrini çıxarın və sürətli yerləşdirmə üçün bütün parametrləri olan sistem şəklinə sahib olun.
8. Tez-tez istifadə olunan proqramların, xüsusən də sistemin təhlükəsizliyini təmin edən proqramların müntəzəm olaraq yenilənməsini həyata keçirin.

Lisenziyalı antivirus proqramları

Ev istifadəsi üçün antivirus seçmək, xüsusən də təcrübəsiz istifadəçilər üçün aktual məsələdir. Gec-tez hər kəs antivirus quraşdırmalıdır. Maraqlı bir faktdır, lakin bir çox istifadəçi kompüterlərini qorumaq üçün proqramlar quraşdırmır. Müxtəlif sistem nasazlıqları yaranana qədər quraşdırmayın. Həqiqətən, kompüter viruslara yoluxduqda, sistem yavaşlayır, kompüter "yavaşlayır" və ya donur. Ən pis halda Trojan proqramları parolları və şəxsi məlumatları oğurlaya bilər. Özünüzü çətinliklərdən qorumaq üçün ev antivirusunu necə seçəcəyini anlamağa çalışaq.

Xüsusilə kompüter və informasiya təhlükəsizliyi ilə

məşğul olan müxtəlif proqram məhsulları istehsalçıları bu gün antivirus proqramlarının geniş seçimini təklif edirlər.

Lisenziyalı antivirus proqramının satın alınması məlumatların icazəsiz girişdən və kompüterdən zərərli məqsədlər üçün istifadəsindən nisbətən etibarlı qorunma təmin edəcək.

Aşağıda İnternet də daxil olmaqla satın alına bilən ən populyar lisenziyalı antivirus proqramları verilmişdir.

Kaspersky Anti-Virus - mobil qurğular üçün versiyalar da daxil olmaqla, HIPS komponentlərini özündə birləşdirən proaktiv mühafizədən istifadə etməklə viruslardan, qurdlardan, troyan atlarından, rootkitlərdən, reklam proqramlarından, casus proqramlardan, o cümlədən naməlum təhlükələrdən real vaxt rejimində müdafiəni təmin edir (18 versiya).

Eset NOD32 - kompüterin tam qorunmasını təmin edir. Kompleks kompüter mühafizəsi real vaxt rejimində işləyir və viruslardan və zərərli proqramlardan, həmçinin fişinq hücumları, qurdlar, casus proqramlar, reklam proqramları və başqaları kimi digər təhlükələrdən etibarlı müdafiəni təmin edir.Fərqləndirici xüsusiyyət resurslardan qənaətlə istifadə edilməsi və yüksək icra sürətidir (31 versiya))

Norton (Symantec) - virusları və casus proqramları bloklayan və İnternetdə təhlükəsiz gəzməyə və məlumat mübadiləsinə imkan verən əsas antivirus müdafiəsi (10 versiya).

Doctor Web virusları və casus proqramları bloklayan və İnternetdə təhlükəsiz şəkildə gəzməyə və məlumat mübadiləsi aparmağa imkan verən əsas antivirus müdafiəsidir (45 müxtəlif versiya).

Avira - AAviraAntivirusPremium - Windows OS ilə

işləyən fərdi kompüterlər üçün virusdan qorunma (18 versiya)

Avast - bu, İnternetə baxarkən daha effektiv qorunmadır, tam xüsusiyyətli antivirus proqramı (23 versiya) .

TrendMicro - Real vaxt yeniləmələri **,** indi və gələcəkdə ən son veb təhlükələrindən qorunma (11 versiya).

AVG (24 versiya)

McAfee - viruslara, casus proqramlara və zərərli proqramlara qarşı effektiv qorunma. Təhlükəsizlik proqramı təhlükəli e-poçt mesajlarını və təhlükəli veb səhifələrin məzmununu daim skan edir və bloklayır (3 versiya).

Ödənişli proqramlara alternativ

Bu gün antivirus proqram istehsalçılarının öz məhsullarının ödənişli həmkarlarından daha az funksional olan pulsuz versiyalarını təklif etmələri qeyri-adi deyil. Bu, bir çox səbəblərə görə edilir, əsas səbəblərdən biri brendinizi istifadəçilər arasında tanıtmaq və populyarlaşdırmaqdır.

Bir qayda olaraq, məhsulun ödənişsiz tam işləməsi üçün onun qeydiyyatı tələb olunur. Adətən bu, əlaqə məlumatlarınızla qeydiyyat formasını doldurmaqdan ibarətdir.

Həmçinin, bəzi antiviruslarda proqramın pullu versiyasını almaq ehtiyacını daim xatırladan bezdirici reklamlar var. Bütün bunlara əlavə olaraq, ödənişsiz antivirus funksionallığı azaldıb. Bütün bunları pulsuz antivirus yükləməklə əldə etmək olar. Ancaq belə məhsullardan istifadə pul tələb etmir!

Qeyd etmək lazımdır ki, bu cür bəzi proqramlar sistemi naməlum və ya az tanınan istehsalçıların kommersiya antiviruslarından daha pis qoruya bilər**.** Beləliklə, antivirusu pulsuz yükləmək və ya antivirusun sınaq versiyasını ödənişli istifadə etmək istifadəçinin özü qərar verir.

Pulsuz antivirus proqramlarına nümunələr:

BitDefenderFreeEdition Antivirus, vaxtaşırı yoxlamalar və skanlar aparmaqla sisteminizi qorumağa kömək edəcək bir proqramdır. İşləyərkən antivirus BitDefender-in ödənişli məhsulları ilə eyni sertifikatlı aşkarlama texnologiyalarından istifadə edir.

Pulsuz antivirus bölməsindən VG Anti-VirusFreeEdition 2013 kompüterin əsas müdafiəsini təmin edəcək**.** Daxili AVG SocialNetworkingProtection sayəsində sosial şəbəkələrdə çox vaxt keçirən ev istifadəçisi üçün yaxşı seçimdir.

Antivirus**!** **FreeAntivirus** pulsuz təhlükəsizlik proqramları arasında ən yaxşı antiviruslardan biridir. Yeni evristik nüvə və yüksək aşkarlama səmərəliliyi Avast-ı bütün dünyada istifadəçilər arasında populyar etdi.

AviraFreeAntivirus həm viruslara, həm də öz işlərində maskalanmadan istifadə edən rootkitlərə qarşı etibarlı müdafiəni təmin edən Alman istehsalçısının antivirusudur.

Comodo sisteminizi viruslardan, casus proqramlardan, rootkitlərdən və digər zərərli proqramlardan qoruyacaq. Antivirusun bəzi xırda xüsusiyyətləri yoxdur, buna görə də pulsuzdur. Daxili avtomatik sandbox funksiyası (AutoSandbox) mövcuddur.

BitDefenderFreeEdition, vaxtaşırı yoxlamalar və skanlar həyata keçirməklə sisteminizi qorumağa kömək

edəcək pulsuz proqramdır. İşləyərkən antivirus BitDefender-in ödənişli məhsulları ilə eyni sertifikatlı aşkarlama texnologiyalarından istifadə edir.

Microsoft -un SecurityEssentials adlı antivirusu viruslardan, casus proqramlardan və digər zərərli proqramlardan qorunma təmin edəcək. Skan jurnalının, planlaşdırıcının və istifadəçilər üçün intuitiv interfeysin olması pulsuz paylanan bu antivirusu bir çox istifadəçilər arasında populyar edib.

RisingAntivirusFreeEdition həm gündəlik iş zamanı, həm də İnternetdə işləyərkən kömək edəcək pulsuz sistem mühafizə proqramıdır. Antivirus sadə və istifadəçi dostu interfeysə, eləcə də bir çox parametrlərə malikdir.

"Zilya" bazarda Ukraynanın təhlükəsizlik üzrə mütəxəssisləri tərəfindən təqdim olunur. Evristik faylların skan edilməsi, poçtun skan edilməsi, böyük antivirus verilənlər bazası və sadə istifadəçi interfeysi bu kifayət qədər gənc antivirusu bir çox istifadəçilər arasında populyarlaşdırmışdır.

d -Aware PULSUZ InternetSecurity pulsuz paylanan və İnternetdə işləyərkən tam qorunma təmin edə bilən antivirusdur. Antivirus funksiyasına əlavə olaraq, proqramda daxili casus proqram aşkarlama modulu var.

PandaCloudAntivirus heç bir xərc çəkmədən Pandadan qabaqcıl müdafiədən istifadə etmək imkanıdır. Antivirus sistemə minimal təsir göstərir və maksimum qoruma təmin edir.

Ev antivirusu seçərkən bütün bu məsələləri həll etməyə vaxtınız və ya istəyiniz yoxdursa, o zaman nüfuzlu müstəqil laboratoriyalar tərəfindən aparılan sınaqların

nəticələrinə əsasən, ev antivirusu konsepsiyasına uyğun gələn iki lider müəyyən edilə bilər. Bu antiviruslar pulsuzdur, sistemi yükləmir, yüksək tarama sürətinə malikdir və yüksək dərəcədə qorunma təmin edir. Bunlar **Avast** antivirusu və **Avira antivirusudur** .

İSTIFADƏ OLUNMUŞ ƏDƏBIYYAT

Azərbaycan dilində

1. V.Ə.Qasımov, Ə.H.Yaqubov "Kompüter mühəndisliyi" Dərslik, Bakı-20212009. 352 səh.
2. V.Ə.Qasımov, İnformasiya təhlükəsizliyi: Kompüter cinayətkarlığı və kiberterrorçuluq", Bakı-2007. 192 səh.
3. V.Ə.Qasımov, İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı-2011. 112 səh.
4. V.Ə.Qasımov, İnformasiya axtarış üsulları və sistemləri. Dərslik. Bakı-2015. 288 səh.
5. Kərimov S.Q., Həbibullayev S.B., Ibrahimзadə T.Ş. – Informatika. Ali məktəblər üçün dərslik. Bakı 2009
6. Əliquliyev R.M., Abdullayeva F.C. Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya texnologiyaları problemləri, 2013
7. Qasımov Vaqif Əlicavad oğlu. İnformasiya təhlükəsizliyinin əsasları. dərslik 2009. -340 s.
8. Salı Şəkərəliyev, Mahmudbəyli Leyla. İnformasiya sistemləri və verilənlər bazası. Bakı 2022
9. Allahverdiyeva N.R. Texniki informatikanın əsasları. Bakı - 2009.
10. Əliyev R.Ə., Salahlı M.Ə. İnformatika və hesablama texnikasının əsasları. Bakı, Maarif, 2004
11. M.N.Əlizadə, H.M.Bayramov, Ə.S.Məmmədov. İnformasiya təhlükəsizliyi, Dərslik, Bakı, 2016 - 384 səh.
12. R.M.Əliquliyev, Y.N.İmamverdiyev Kriptoqrafiyanın əsasları" Bakı - 2006

13. R. M. Əliquliyev, Y. N. İmamverdiyev “Rəqəm imzası texnologyası” Bakı – Elm – 2003

Rus dilində:

1. Операционные системы : учебник для студ. учреждений высш. проф. образования/ С.В.Синицын, А.В.Батаев,. Н.Ю.Налютин. — 3-е изд., 2021
2. Ю.Д.Романова Информатика и информационные технологии : учеб. пособие для студентов ; под ред.Ю.Д.Романовой М. : Эксмо, 2015
3. Основы безопасности информационных систем : Учебное пособие для вузов по специальности "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем" /Д. П. Зегжда, А. М. Ивашко

İnternet resursları:

1. https://www.bmstu.ru/
2. https:www.microsoft.com
3. https:www.gadirov.com
4. https://az.wikipedia.org/wiki
5. http://www.viruslist.com
6. http://www.bytemag.ru
7. http://www.wasm.ru
8. http://abisoft.ru
9. http://antivibest.ru
10. http://sdu-sdtk.edu.az/

Müəlliflər haqqında məlumat

Salayev Oktay Ağacan oğlu 1976-cı il dekabr ayının 19-da Bakı şəhərində anadan olub.

1997-ci ildə Bakı Ali Birləşmiş Komandirlər Məktəbini taktiki rabitə qoşunları komandiri ixtisası (mülki ixtisas - elektrikli rabitə vasitələri üzrə mühəndis) üzrə bitirib. 1997-2014 tarixlərdə Müdafiə Nazirliyinin hərbi hissələrində müxtəlif vəzifələrdə xidmət edib.

1999-cu ildə NATO zabitlərin təkmilləşdirmə kursunu, 2016-cı ildə Azərbaycan Pedoqoji Universiteti, Gənclərin çağırışaqədərki hazırlıq rəhbərlərinin ixtisasartırma kursunu, 2017-ci ildə Mülki Müdafiə İdarəsinin Mərkəzi Mülki Müdafiə kursunu bitirib.

2015-ci ildən Azərbaycan Texniki Universiteti nəzdində Bakı Dövlət Rabitə və Nəqliyyat Kollecində hərbi hazırlıq rəhbəri vəzifəsində çalışır.

13 dərsliyin, 2 dərs vəsaitinin və 8 ixtisas üzrə tədris proqramının müəllifidir.

Rəhimov Nurlan Kərim oğlu 1998-ci il avqust ayının 1-də Sabirabad rayonu Suqovuşan kəndində anadan olub. 2015-ci ildə Azərbaycan Dövlət Pedaqoji Universitetinin "və informatika" fakültəsini bitirib.

2021-ci ildən Sabirabad Dövlət Sosial-İqtisadi kollecində Riyaziyyat və İnformatika müəllimi vəzifəsində çalışır.

Mirzəyeva Günel Mahir qızı 1986-cı il dekabr ayının 24-də Sabirabad şəhərində anadan olub.

2008-ci ildə Bakı Dövlət Universitetini "Fizika" ixtisası üzrə bitirib.

2009 cu ildə Azərbaycan Dövlət Pedaqoji Universitetini "Riyaziyyat və İnformatika" ixtisası üzrə yenidənhazırlanma təhsilinin tam kursunu bitirib.

2010-cu ildən Azərbaycan Texniki Universiteti nəzdində Bakı Dövlət Rabitə və Nəqliyyat Kollecində "Ümumtəhsil" fənn birləşməsi komissiyasında müəllim vəzifəsində çalışır.

2 dərsliyin və 3 ixtisas üzrə fənn proqramının müəllifidir.

Salayev Oktay Ağacan
Rəhimov Nurlan Kərim
Mirzəyeva Günel Mahir

İnformasiya sistemlərində təhlükəsizliyin təmini

Orta ixtisas təhsili müəssisələrinin tələbələri üçün dərslik

Müəlliflik hüquqları qorunur. Xüsusi icazə olmadan bu nəşri və yaxud onun hər hansı hissəsini yenidən çap etdirmək, surəti çıxartmaq, elektron informasiya vasitərləri ilə yaymaq qanuna ziddir. Bu dərsliklə bağlı irad və təkliflərinizi oktay.salayev@gmail.com elektron ünvanına göndərməyiniz xahiş olunur. Əməkdaşlığınız üçün əvvəlcədən təşəkkür edirik!

Naşir: Mayıl Mayılov
Dizayner: Jalə Əliyeva
Texniki redaktor: Arzu Salayeva
Korrektor: Zeynəb Salayeva

Yığılmağa verilmişdir: 22.02.2024.
Çapa imzalanıb: 25.02.2024
Hesab – nəşriyyat həcmi. Fiziki çap vərəqi 19.
Formatı 60x84 1/16. Səhifə 156. Ofset kağızı. Ofset çapı.
Tiraj 300 nüsxə, Qiyməti müqavilə ilə. "CLASS PRİNT MMC" mətbəəsində çap olunmuşdur.
Tel.: +994 55 640 00 94