TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

DOI: https://doi.org/10.36719/2663-4619/103/146-153

Ramazan Eyyubov
Odlar Yurdu Universiteti
riyaziyyat üzrə fəlsəfə doktoru
eyyubov54@mail.ru
İlham Cəbrayılov
Odlar Yurdu Universiteti
ilham_cabrayilov@mail.ru
Həcər Əfəndiyeva
Odlar Yurdu Universiteti
hecer.efendy@gmail.com
Sevda Abulova
Hədəf liseyi
seva-abulova@mail.ru

İNFORMASİYA TƏHLÜKƏSİZLİYİ NƏZƏRİYYƏSİNİN ƏSAS MÜDDƏALARI VƏ TƏHLÜKƏSİZLİK HÜCUMLARININ TƏSNİFATI

Xülasə

XXI əsrin başlanğıcı insan inkişafının bütün sahələrində informasiya texnologiyalarının sürətli inkişafı ilə əlamətdardır. Eyni zamanda informasiya getdikcə daha çox strateji resursa, məhsuldar qüvvəyə və bahalı əmtəəyə çevrilir. Kompüter sistemləri və şəbəkə texnologiyaları sürətlə inkişaf edir. Müvafiq olaraq, informasiyanı qorumaq üçün yeni üsullar da sürətlə ortaya çıxır. İnformasiyanın qorunması və onun təhlükəsizliyinin etibarlı təminatı məsələsi dövrümüzün ən mühüm problemlərindən biridir. Buna görə də mövzu çox aktualdır.

Kompüter sistemlərinin unifikasiyası, qlobal şəbəkələrin yaradılması və informasiya resurslarının çıxış imkanlarının genişləndirilməsinə səbəb olur. Proqram təminatının mürəkkəbliyinin artması və bununla əlaqədar onların etibarlılığının azalması və zəifliklərin sayının artmasına səbəb olur. Kompüter şəbəkələri spesifik təbiətinə görə, sadəcə olaraq, informasiya təhlükəsizliyi problemlərinə məhəl qoymadan normal fəaliyyət göstərə və inkişaf edə bilməyəcəklər.

Açar sözlər: *kompüter, şəbəkə, təhlükəsizlik, informasiya texnologiyaları, təhdid, kompüter sistemi, məlumat, kompüter sisteminə hücum*

Ramazan Eyyubov
Odlar Yurdu University
Doctor of Philosophy in Mathematics
eyyubov54@mail.ru
Ilham Jabrayilov
Odlar Yurdu University
ilham_cabrayilov@mail.ru
Hajar Efendiyeva
Odlar Yurdu University
hecer.efendy@gmail.com
Sevda Abulova
Hedef Lyceum
seva-abulova@mail.ru

Basic provisions of information security theory and classification of security attacks

Abstract

The beginning of the twenty-first century is marked by the rapid development of information technologies in all areas of human development. At the same time, information is increasingly becoming a strategic resource, a productive force, and an expensive commodity. Computer systems and network technologies are developing very rapidly. Accordingly, new methods for protecting information are also emerging rapidly. The problem of information protection and reliable provision of its security is one of the most important problems of our time. Therefore, the topic is very relevant.

The unification of computer systems leads to the creation of global networks and expansion of access to information resources. The increase in the complexity of software leads to a decrease in their reliability and an increase in the number of vulnerabilities. Computer networks, due to their specific nature, simply cannot function and develop normally without ignoring information security issues.

Keywords: *computer, network, security, information technology, threat, computer system, information, computer system attack*

Giriş

I. İnformasiya təhlükəsizliyi nəzəriyyəsinin əsas müddəaları

1.1 *İnformasiya təhlükəsizliyi təhdidlərinin təsnifatı*

Kompüter şəbəkəsində (KŞ) məlumatın təhlükəsizliyinə təhdid, orada işlənən məlumatın təhlükəsizliyinin pozulması ilə əlaqəli KŞ-nin işində dəyişiklik yarada biləcək bir hadisə və ya hərəkət kimi başa düşülür.

İnformasiya zəifliyi informasiya təhlükəsizliyinə təhdidlərin həyata keçirilməsi üçün şəraitin yarandığı şəraitin mümkünlüyüdür.

Kompüter sisteminə hücum, müəyyən bir zəifliyi axtarmaq və ondan istifadə etməkdən ibarət olan təcavüzkar tərəfindən həyata keçirilən bir hərəkətdir. Başqa sözlə, kompüter sisteminə hücum onda olan məlumatların təhlükəsizliyinə təhlükənin həyata keçirilməsidir.

Kompüter şəbəkələrində işləyərkən məlumat ötürülməsinin təhlükəsizliyi ilə bağlı yaranan problemləri üç əsas növə bölmək olar (Kasperski, 2013):

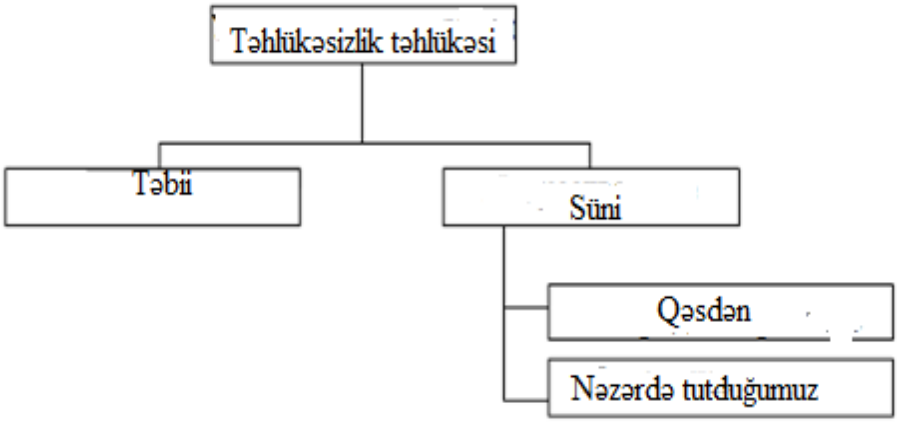
- informasiyanın ələ keçirilməsi – məlumatın bütövlüyü qorunur, lakin onun məxfiliyi pozulur;
- məlumatın dəyişdirilməsi – ilkin mesaj dəyişdirilir və ya tamamilə başqası ilə əvəz edilir və ünvana göndərilir;
- məlumat müəllifliyinin dəyişdirilməsi. Bu problem ciddi nəticələrə səbəb ola bilər.

Məsələn, kimsə başqasının adı ilə məktub göndərə bilər (bu cür aldatma adətən *spoofing* adlanır) və ya Web server özünü elektron mağaza kimi göstərə bilər, sifarişləri, kredit kart nömrələrini qəbul edə bilər, lakin heç bir mal göndərə bilməz.

Kompüter şəbəkələrinin həssaslığı nöqteyi-nəzərdən spesifikliyi, əsasən, coğrafi cəhətdən səpələnmiş və heterojen (müxtəlif) elementlər arasında intensiv informasiya qarşılıqlı əlaqəsinin olması ilə bağlıdır.

KŞ-nin sözün əsl mənasında bütün əsas struktur və funksional elementləri həssasdır: iş stansiyaları, serverlər (Host maşınlar), şəbəkə körpüləri (şlüzlər, keçid mərkəzləri), rabitə kanalları və s.

İnformasiya təhlükəsizliyinə müxtəlif mənşəli çoxlu sayda müxtəlif təhdidlər mövcuddur. Ədəbiyyatda müxtəlif təsnifatlar mövcuddur ki, burada bölünmə meyarı kimi yaranan təhlükələrin növləri, zərərli niyyətin dərəcəsi, təhlükə mənbələri və s. Ən sadə təsnifatlardan biri aşağıdakı şəkildə göstərilmişdir (2) (Şəkil 1.).



Şəkil 1. Təhlükəsizlik təhdidlərinin ümumi təsnifatı

Təbii təhlükələr KŞ və onun obyektiv fiziki proseslərin elementlərinə və ya insanlardan asılı olmayaraq təbii hadisələrə təsir nəticəsində yaranan təhlükələrdir.

Texnogen təhlükələr, insan fəaliyyəti nəticəsində yaranan KŞ üçün təhlükələrdir. Onların arasında, hərəkətlərin motivasiyasına əsaslanaraq qeyd edə bilərik:

- KŞ-nin və onun elementlərinin layihələndirilməsində səhvlər, proqram təminatındakı səhvlər, personalın hərəkətlərindəki səhvlər və s. nəticəsində yaranan qəsdən (qəsdən, təsadüfi) təhlükələr;
- insanların (hücum edənlərin) eqoist istəkləri ilə əlaqəli qəsdən təhdidlər, insanların (hücum edənlərin) istəkləri.

KŞ ilə əlaqəli təhlükə mənbələri xarici və ya daxili ola bilər (KŞ-nin özünün komponentləri – onun avadanlıqları, proqramları, personalı).

Təhdidlərin həyata keçirilməsinin mənfi nəticələrinin təhlili mümkün təhlükə mənbələrinin, onların təzahürünə kömək edən zəifliklərin və həyata keçirilmə üsullarının məcburi müəyyən edilməsini tələb edir.

Cədvəl.
İnformasiya təhlükəsizliyi təhdidlərinin həyata keçirilməsi modeli

Təhlükə	**Hücum**		
Oğurluq	Təhlükənin mənbələri	Zəifliklər	Təhlükənin həyata keçirilməsi metodu
Zərər	Antropoloji (nəzərdə tutulan)	Obyektiv	Analtik
Bloklama	Texnoloji	Subyektiv	Texniki
Məhvetmə	Təbii	Təsadüfi	Proqramlarla
Modifikasiya			Sosial
Həqiqiliyin inkarı			Təşkil edilmiş
Yalanın tətbiqi			
	Zəifləmənin aradan qaldırılması		
	Müdafiə metodları		Təhlükənin həyata keçirilməsinin nəticəsi
	Fəlakətli		Sahibinə dəyən ziyan
	Təşkilati		
	Texniki		
	Mühəndis-texniki		
	Proqram apparatı		

Təhdidlər təhlükəsizlik məqsədlərinin pozulması halında münasibətlərin subyektinə zərər vurma ehtimalına görə təsnif edilir (Domarev, 2012). Zərər hansısa subyekt tərəfindən (cinayət, təqsir və ya səhlənkarlıq) səbəb ola bilər, həmçinin təzahürlərin predmetindən asılı olmayan nəticəyə çevrilə bilər. Təhdidlər o qədər də çox deyil. Məlumatın məxfiliyini təmin edərkən bura məlumatın və onun emal vasitələrinin oğurlanması (kopyalanması), habelə onun itirilməsi (qəsdən itirilməsi, sızması) daxil ola bilər. İnformasiyanın bütövlüyü təmin edilərkən təhlükələrin siyahısı aşağıdakı kimidir: məlumatın dəyişdirilməsi (təhrif edilməsi); məlumatın həqiqiliyinin inkar edilməsi; yalan məlumatların tətbiqi. İnformasiyanın mövcudluğunu təmin edərkən onu bloklamaq, yaxud məlumatın özünü və onun emal vasitələrini məhv etmək mümkündür.

Bütün təhlükə mənbələrini medianın növünə görə siniflərə, sinifləri isə yerləşdiyi yerə görə qruplara bölmək olar. Zəifliklər, həmçinin zəifliklərin mənbəyinə görə siniflərə, təzahürlərinə görə isə qruplara və alt qruplara bölünə bilər. İcra üsullarını icra üsullarına görə qruplara bölmək olar. Nəzərə almaq lazımdır ki, "metod" anlayışının özü yalnız antropogen mənbələrdən gələn təhlükələrin həyata keçirilməsini nəzərdən keçirərkən tətbiq olunur. Texnogen və təbii mənbələr üçün bu anlayış "ilkin şərt" anlayışına çevrilir (Mostovoy, 2010). Təhdidlərin (hücumların) həyata keçirilməsi imkanlarının təsnifatı, hücum məqsədlərinin həyata keçirilməsinə səbəb olan zəifliklərdən istifadə edərək müəyyən həyata keçirmə üsullarından istifadə edərək təhlükə mənbəyinin hərəkətləri üçün mümkün variantlar toplusudur. Hücumun məqsədi təhlükənin həyata keçirilməsi məqsədi ilə üst-üstə düşməyə bilər və təhlükənin sonrakı həyata keçirilməsinə nail olmaq üçün zəruri olan ara nəticə əldə etməyə yönəlmiş ola bilər. Belə uyğunsuzluq halında, hücum təhlükənin həyata keçirilməsinə yönəlmiş hərəkətlərin görülməsinə hazırlıq mərhələsi kimi qəbul edilir, yəni qanunsuz hərəkəti "törətməyə hazırlıq" kimi. Hücumun nəticəsi təhlükənin həyata keçirilməsi və ya belə həyata keçirilməsinə töhfə verən nəticələrdir.

Şəbəkədə işləyərkən təhlükəsizlik təhdidlərinin qiymətləndirilməsi və təhlili üçün ilkin məlumatlar, onların fəaliyyət istiqamətlərini, təhlükəsizlik məqsədlərinin gözlənilən prioritetlərini, şəbəkədə həll olunan vəzifələri və həyata keçirmək üçün şərtləri anlamağa yönəlmiş münasibətlər subyektləri arasında sorğunun nəticələridir.

Ən tez-tez və ən təhlükəli (zərər miqdarı baxımından) adi istifadəçilərin, operatorların, sistem administratorlarının və kompüter şəbəkəsinə qulluq edən digər şəxslərin qəsdən səhvləridir (Shan'gin, 2012). Bəzən belə səhvlər, əslində, təhdidlərdir (səhv daxil edilmiş məlumatlar və ya sistemin çökməsinə səbəb olan proqram xətası), bəzən onlar təcavüzkarlar tərəfindən istifadə edilə bilən zəifliklər yaradır (bunlar adətən inzibati xətalardır). Bəzi hesablamalara görə, itkilərin 65 %-ə qədəri qəsdən səhvlərin nəticəsidir.

Yanğınlar, daşqınlar işdə savadsızlıq və səhlənkarlıq qədər bəla gətirmir.

Aydındır ki, istəmədən səhvlərlə mübarizənin ən radikal yolu maksimum avtomatlaşdırma və ciddi nəzarətdir.Digər əlçatanlıq təhlükələri, təhdidlərin hədəf aldığı kompüter sisteminin komponentlərinə görə təsnif edilə bilər:

- istifadəçinin imtinası,
- daxili şəbəkənin nasazlığı,
- dəstəkləyici infrastrukturun uğursuzluğu.

Bir qayda olaraq, istifadəçilərlə bağlı aşağıdakı təhlükələr nəzərə alınır:

- informasiya sistemi ilə işləmək istəməməsi (ən çox yeni imkanları mənimsəmək lazım olduqda və istifadəçi sorğuları ilə faktiki imkanlar və texniki xüsusiyyətlər arasında uyğunsuzluq olduqda özünü göstərir),
- müvafiq təlimin olmaması səbəbindən sistemlə işləyə bilməmək (ümumi kompüter savadının olmaması, diaqnostik mesajları şərh edə bilməməsi, sənədlərlə işləmək bacarığının olmaması və s.),
- texniki dəstəyin olmaması səbəbindən sistemlə işləyə bilməmək (natamam sənədlər, arayış məlumatlarının olmaması və s.).

Daxili uğursuzluqların əsas mənbələri bunlardır:

- müəyyən edilmiş istismar qaydalarından kənara çıxma (təsadüfən və ya qəsdən),

- istifadəçilərin və ya texniki xidmət işçilərinin təsadüfi və ya qəsdən hərəkətləri (sorğuların təxmini sayından artıq olması, işlənmiş məlumatların həddindən artıq həcmi və s.) nəticəsində sistemin normal iş rejimindən çıxması,
- sistemin (yenidən) konfiqurasiyası zamanı xətalar,
- proqram təminatı və avadanlıqların nasazlığı,
- məlumatların məhv edilməsi,
- avadanlıqların məhv edilməsi və ya zədələnməsi.

Dəstəkləyici infrastrukturla bağlı aşağıdakı təhlükələri nəzərə almaq tövsiyə olunur:

- rabitə sistemlərinin, enerji təchizatının, su və ya istilik təchizatının, kondisionerin (təsadüfən və ya qəsdən) pozulması;
- binaların məhv edilməsi və ya zədələnməsi;
- xidmət personalının və ya istifadəçilərin öz vəzifələrini yerinə yetirə bilməməsi və ya istəməməsi (vətəndaş iğtişaşları, nəqliyyat qəzaları, terror aktı və ya onun təhlükəsi, tətil və s.).

Sözdə "incimiş" işçilər – indiki və keçmiş – çox təhlükəlidirlər. Bir qayda olaraq, təşkilata zərər verməyə çalışırlar – "cinayətkar".

Misal üçün:

- zədələnmiş avadanlıq,
- proqramları və yaxud məlumatları sonda məhv edəcək məntiq bombası qurmaq,
- məlumatları silin.

İncimiş işçilər, hətta keçmiş işçilər, təşkilatdakı prosedurlarla tanışdırlar və xeyli ziyan vurmağa qadirdirlər. Təmin etmək lazımdır ki, işçi işdən çıxdıqda onun informasiya resurslarına çıxış hüquqları (məntiqi və fiziki) ləğv edilsin (Panasenko, 2013).

1.2. *CS-nin təhlükəsizliyinə qəsdən təhdidlərin növləri*

Passiv təhdidlər əsasən şəbəkə informasiya ehtiyatlarının işinə təsir etmədən icazəsiz istifadəyə yönəlib. Məsələn, verilənlər bazasına icazəsiz daxil olmaq, rabitə kanallarını dinləmək və s.

Aktiv təhlükələr şəbəkənin komponentlərini hədəf alaraq onun normal fəaliyyətini pozmaq məqsədi daşıyır. Aktiv təhlükələrə, məsələn, kompüterin və ya onun əməliyyat sisteminin sıradan çıxması, verilənlər bazasında məlumatların təhrif edilməsi, kompüter proqramlarının məhv edilməsi, rabitə xətlərinin pozulması və s. aiddir. Aktiv təhlükələr hakerlər, zərərli proqramlar və s. vasitəsilə meydana gəlir (Romanets, 2013: 30).

Qəsdən təhdidlər daxili və xarici olaraq iki yerə bölünür.

Xarici mənbələrin məlumatına görə, sənaye casusluğu geniş vüsət alıb – bu, kommersiya sirrini təşkil edən məlumatların onun sahibi tərəfindən icazə verilməyən şəxs tərəfindən qanunsuz olaraq toplanması, mənimsənilməsi və ötürülməsi kommersiya sirri sahibinə ziyan vurur.

İnformasiya təhlükəsizliyi və şəbəkənin normal işləməsi üçün əsas təhdidlərə aşağıdakılar daxildir:

- məxfi məlumatların sızması,
- məlumatın kompromisi,
- informasiya ehtiyatlarından icazəsiz istifadə,
- informasiya resurslarından səhv istifadə,
- abunəçilər arasında icazəsiz məlumat mübadiləsi,
- məlumatdan imtina,
- informasiya xidmətlərinin pozulması,
- imtiyazlardan qeyri-qanuni istifadə.

Məxfi məlumatın sızması məxfi məlumatın şəbəkədən və ya xidmət vasitəsilə etibar edildiyi və ya iş zamanı məlum olan istifadəçilərin dairəsindən kənara nəzarətsiz buraxılmasıdır.

Məlumatın sahibi tərəfindən açıqlanması — xidməti və ya işi ilə müəyyən edilmiş qaydada müvafiq məlumat həvalə edilmiş vəzifəli şəxslərin və istifadəçilərin qəsdən və ya ehtiyatsızlıqdan hərəkətləridir ki, bu da həmin şəxslərin məlumatla tanış olmasına səbəb olur. (Khoreyev, 2013).

İcazəsiz giriş qorunan məlumatlara daxil olmaq hüququ olmayan şəxs tərəfindən məxfi məlumatın qanunsuz olaraq qəsdən əldə edilməsidir.

İnformasiyaya icazəsiz girişin ən çox yayılmış üsulları bunlardır:

- elektron şüalanmanın tutulması,
- parazit daşıyıcı modulyasiyasını əldə etmək üçün rabitə xətlərinin məcburi elektromaqnit şüalanması (işıqlandırılması),
- dinləmə cihazlarından (əlfəcinlərdən) istifadə,
- uzaqdan çəkiliş,
- akustik şüalanmanın tutulması və printer mətninin bərpası,
- icazə verilən sorğuları yerinə yetirdikdən sonra sistem yaddaşında qalıq məlumatların oxunması,
- təhlükəsizlik tədbirlərini aşaraq yaddaş daşıyıcılarının surətinin çıxarılması,
- qeydiyyatdan keçmiş istifadəçi kimi maskalanmaq,
- sistem sorğuları kimi maskalamaq,
- proqram tələlərindən istifadə,
- proqramlaşdırma dillərinin və əməliyyat sistemlərinin çatışmazlıqlarından istifadə etmək,
- informasiyaya çıxışı təmin edən xüsusi hazırlanmış texniki vasitələrin avadanlıq və rabitə xətlərinə qanunsuz qoşulma,
- mühafizə mexanizmlərinin zərərli şəkildə söndürülməsi,
- şifrələnmiş informasiyanın xüsusi proqramlar vasitəsilə deşifrə edilməsi,
- informasiya infeksiyaları (Sidorin, 2013: 39).

Məxfi məlumatı sızdırmaq üçün istənilən vasitə həm şəbəkənin fəaliyyət göstərdiyi təşkilata, həm də onun istifadəçilərinə əhəmiyyətli maddi və mənəvi ziyan vura bilər.

Zərərli proqram təminatı

Hücumların həyata keçirilməsinin ən təhlükəli üsullarından biri hücuma məruz qalan sistemlərə zərərli proqram təminatının daxil edilməsidir.

Bölüşmə mexanizminə görə onlar fərqləndirilir:

Məntiqi – məlumatı təhrif etmək və ya məhv etmək üçün daha az istifadə olunur, oğurluq və ya fırıldaqçılıq üçün istifadə olunur; Məntiq bombası manipulyasiyası adətən təşkilatı tərk etməyi planlaşdıran narazı işçilər tərəfindən edilir.

Məntiq bombasının əsl nümunəsi: işdən çıxarılmasını gözləyən bir proqramçı əmək haqqı proqramında müəyyən dəyişikliklər edir, adı şirkətin kadr məlumat dəstindən itdikdən sonra qüvvəyə minməyə başlayır.

Trojan atı, əsas, yəni tərtib edilmiş və sənədləşdirilmiş hərəkətlərə əlavə olaraq, sənədlərdə təsvir olunmayan əlavə hərəkətləri yerinə yetirən bir proqramdır. Qədim Yunan Troya atı ilə bənzətmə haqlıdır – hər iki halda təhlükə, şübhəsiz, bir qabıqda gizlənir. Trojan atı bu və ya digər şəkildə orijinal zərərsiz proqrama daxil edilmiş, sonradan şəbəkə istifadəçilərinə ötürülən (bağışlanan, satılan, dəyişdirilən) əlavə əmrlər blokudur. Bu əmrlər bloku müəyyən bir vəziyyət yarandıqda (tarix, vaxt, xarici əmrlə və s.) işə salına bilər.

Belə bir proqramı işə salan hər kəs həm öz fayllarını, həm də bütövlükdə bütün CS fayllarını təhlükə qarşısında qoyur. Troyan atı, adətən, bir istifadəçinin səlahiyyətləri çərçivəsində, lakin başqa istifadəçinin və ya hətta şəxsiyyətini müəyyən etmək bəzən qeyri-mümkün olan yad birinin maraqlarına uyğun hərəkət edir.

Trojan atı onu işə salan istifadəçinin geniş imtiyazlar dəsti varsa, ən təhlükəli hərəkətləri edə bilər. Bu halda, Trojan atını yaradan və təqdim edən və özü bu imtiyazlara malik olmayan təcavüzkar icazəsiz imtiyazlı funksiyalar yerinə yetirə bilər.

Virus, daha çoxalma qabiliyyətinə malik olan dəyişdirilmiş nüsxəni daxil etməklə digər proqramları yoluxdura bilən proqramdır (Goshko, 2014: 93).

Virusun iki əsas xüsusiyyətlə xarakterizə olunduğu güman edilir:

- özünü çoxaltma qabiliyyəti,
- hesablama prosesinə müdaxilə etmək bacarığı.

Son illərdə viruslarla mübarizə problemi çox aktuallaşıb, buna görə də bir çox insan bunun üzərində işləyir. Müxtəlif təşkilati tədbirlər tətbiq edilir, yeni antivirus proqramlarından istifadə edilir və bütün bu tədbirlər təbliğ olunur. Son zamanlar yoluxma və məhvetmə miqyasını az və ya

çox məhdudlaşdırmaq mümkün olmuşdur. Lakin canlı təbiətdə olduğu kimi, bu mübarizədə də tam uğur əldə edilməmişdir.

Qurd şəbəkə vasitəsilə yayılan və özünün surətini maqnit mühitində qoymayan proqramdır. Qurd hansı hostun yoluxmuş ola biləcəyini müəyyən etmək üçün şəbəkə dəstək mexanizmlərindən istifadə edir. Daha sonra eyni mexanizmlərdən istifadə edərək bədənini və ya bir hissəsini bu düyünə köçürür və ya işə salır, ya da bunun üçün uyğun şərtləri gözləyir. Bu sinfin ən məşhur nümayəndəsi 1988-ci ildə interneti yoluxdurmuş *Morris* virusudur. Qurdun yayılması üçün uyğun mühit bütün istifadəçilərin dost hesab edildiyi və bir-birinə güvəndiyi, qoruyucu mexanizmlərin olmadığı şəbəkədir. Özünüzü bir qurddan qorumağın ən yaxşı yolu şəbəkənizə icazəsiz girişə qarşı tədbir görməkdir.

Şifrə oğurlayanlar parolları oğurlamaq üçün xüsusi olaraq hazırlanmış proqramlardır. İstifadəçi sistem terminalına daxil olmağa çalışdıqda, iş sessiyasını bitirmək üçün lazım olan məlumat ekranda göstərilir. Daxil olmağa cəhd edərkən istifadəçi işğalçının sahibinə göndərilən ad və parol daxil edir, bundan sonra səhv mesaj göstərilir, giriş və idarəetmə əməliyyat sisteminə qaytarılır. Parolunu yazarkən səhv etdiyini düşünən istifadəçi yenidən sistemə daxil olur və sistemə giriş əldə edir. Lakin onun adı və şifrəsi artıq işğalçı proqramının sahibinə məlumdur. Parolun tutulması başqa yollarla da mümkündür. Bu təhlükənin qarşısını almaq üçün sistemə daxil olmamışdan əvvəl ad və şifrəni başqa bir proqrama deyil, xüsusi olaraq sistem daxiletmə proqramına daxil etdiyinizə əmin olmalısınız. Bundan əlavə, parollardan istifadə və sistemlə işləmək qaydalarına ciddi riayət etməlisiniz. Əksər pozuntular ağıllı hücumlara görə deyil, əsas səhlənkarlığa görə baş verir. Parollardan istifadə üçün xüsusi hazırlanmış qaydalara riayət etmək etibarlı qorunmanın zəruri şərtidir (Yakimenko, 2013).

Məlumatın kompromissi

O, bir qayda olaraq, verilənlər bazasında icazəsiz dəyişikliklər yolu ilə həyata keçirilir. Bunun nəticəsində istehlakçısı ya ondan imtina etməyə, ya da dəyişiklikləri müəyyən etmək və həqiqi məlumatı bərpa etmək üçün əlavə səylər göstərməyə məcbur olur. Təhlükəli məlumatlardan istifadə edərkən istehlakçı səhv qərarlar vermək riski altındadır.

İnformasiya resurslarından icazəsiz istifadə bir tərəfdən onun sızmasının nəticələri və ona güzəşt vasitəsi, digər tərəfdən müstəqil əhəmiyyət kəsb edir, çünki idarə olunan sistemə (tam uğursuzluğa qədər) və ya onun abunəçilərinə böyük ziyan vura bilər.

İcazə verildiyi halda informasiya ehtiyatlarının səhv istifadəsi qeyd olunan resursların məhvinə, sızmasına və ya güzəştə getməsinə səbəb ola bilər. Bu təhlükə çox vaxt CS-də istifadə olunan proqram təminatındakı səhvlərin nəticəsidir.

Abunəçilər arasında icazəsiz məlumat mübadiləsi onlardan birinin ona daxil olması qadağan edilən məlumatı alması ilə nəticələnə bilər. Nəticələr icazəsiz giriş üçün olduğu kimidir.

İcazə verildiyi halda, məlumat ehtiyatlarının istifadəsi qeyd olunan resursların məhvinə, sızmasına və ya təsirinə səbəb ola bilər. Bu təhlükə çox vaxt CS-də istifadə edilən proqramdan istifadə edilən səhvlərin aradan qaldırılmasıdır.

Abunəçilər arasında icazəsiz məlumat əldə etmək onlardan birinin ona daxil olması ilə əlaqədar məlumat əldə etmək olar. Nəticələr icazəsiz giriş üçün olduğu kimidir.

Məlumatdan imtina bu məlumatı alan və ya göndərən tərəfindən onun alınması və ya göndərilməsi faktlarının tanınmamasından ibarətdir. Bu, tərəflərdən birinə rəsmi şəkildə imtina etmədən bağlanmış maliyyə müqavilələrini texniki yolla ləğv etməyə və bununla da digər tərəfə xeyli ziyan vurmağa imkan verir.

İnformasiya xidmətinin pozulması təhlükədir, onun mənbəyi CS-də istifadə olunan İT-dir. Abunəçiyə informasiya resurslarının verilməsində gecikmə onun üçün ağır nəticələrə səbəb ola bilər. İstifadəçinin qərar qəbul etmək üçün lazım olan məlumatların vaxtında olmaması onun irrasional hərəkət etməsinə səbəb ola bilər.

İmtiyazlardan qeyri-qanuni istifadə

Hər hansı qorunan sistem fövqəladə hallarda istifadə olunan alətləri və ya mövcud təhlükəsizlik siyasətini pozaraq fəaliyyət göstərə bilən alətləri ehtiva edir. Məsələn, gözlənilməz audit zamanı

istifadəçi sistemin bütün dəstlərinə daxil ola bilməlidir. Bu alətlər adətən administratorlar, operatorlar, sistem proqramçıları və xüsusi funksiyaları yerinə yetirən digər istifadəçilər tərəfindən istifadə olunur.

Əksər təhlükəsizlik sistemləri belə hallarda imtiyaz dəstlərindən istifadə edir, yəni müəyyən funksiyanı yerinə yetirmək üçün müəyyən imtiyaz tələb olunur. Tipik olaraq, istifadəçilərin minimum imtiyazlar dəsti var, idarəçilər isə maksimuma malikdir.

İmtiyaz dəstləri təhlükəsizlik sistemi ilə qorunur. İmtiyazların icazəsiz (qanunsuz) ələ keçirilməsi təhlükəsizlik sistemində səhvlər olduqda mümkündür, lakin ən çox təhlükəsizlik sisteminin idarə edilməsi prosesində, xüsusən də imtiyazlardan ehtiyatsız istifadə edildikdə baş verir (Mel'nikov, 2011: 113).

Təhlükəsizlik sisteminin idarə edilməsi qaydalarına ciddi riayət etmək və minimum imtiyazlar prinsipinə riayət etmək bu cür pozuntuların qarşısını almağa imkan verir.

Nəticə

İnformasiyanın emalı proseslərinin avtomatlaşdırılması vasitələri, üsulları və formaları inkişaf etdikcə və mürəkkəbləşdikcə onun zəifliyi artır. Bu gün, yəqin ki, heç kim informasiyaya icazəsiz girişlə bağlı kompüter cinayətlərindən ümumi itkilərin dəqiq rəqəmini deyə bilməz. Bu, ilk növbədə, zərər çəkmiş şirkətlərin öz itkiləri barədə ictimaiyyətə məlumat vermək istəməməsi, həmçinin məlumatların oğurlanması nəticəsində yaranan itkilərin həmişə pul baxımından dəqiq qiymətləndirilə bilməməsi ilə izah olunur.

Kompüter cinayətlərinin və bununla bağlı maliyyə itkilərinin intensivləşməsinin bir çox səbəbləri var, bunlardan ən əhəmiyyətliləri:

- informasiyanın saxlanması və ötürülməsi üçün ənənəvi "kağız" texnologiyasından elektron texnologiyaya keçid və belə texnologiyalarda informasiya təhlükəsizliyi texnologiyasının kifayət qədər inkişafı;
- kompüter sistemlərinin unifikasiyası, qlobal şəbəkələrin yaradılması və informasiya resurslarına çıxış imkanlarının genişləndirilməsi;
- proqram təminatının mürəkkəbliyinin artması və bununla əlaqədar onların etibarlılığının azalması və zəifliklərin sayının artması.

Kompüter şəbəkələri spesifik təbiətinə görə, sadəcə olaraq informasiya təhlükəsizliyi problemlərinə məhəl qoymadan normal fəaliyyət göstərə və inkişaf edə bilməyəcəklər.

Ədəbiyyat

1. Kasperski, K. (2013). Zapiski issledovatelya komp'yuternykh virusov. Piter.
2. Grishina, N. V. Organizatsiya kompleksnoy zashchity informatsii. http://citforum.ru
3. Domarev, V. V. (2012). Zashchita informatsii i bezopasnost' komp'yuternykh sistem. Piter.
4. Mostovoy, D. Yu. (2010). Sovremennyye tekhnologii bor'by s virusami. Mir.
5. Shan'gin, V. (2012). Zashchita komp'yuternoy informatsii.
6. Panasenko, A. (2013). Sovremennyye metody i sredstva zashchity ot vnutrennikh narushiteley. DialogNauka.
7. Romanets, Yu. V. (2013). Zashchita informatsii v komp'yuternykh sistemakh i setyakh.
8. Khoreyev, P. B. (2013). Metody i sredstva zashchity informatsii v komp'yuternykh sistemakh. Moskva: Akademiya.
9. Sidorin, Yu. S. (2013). Tekhnicheskiye sredstva zashchity informatsii. MGTU im. Baumana.
10. Goshko, S. V. (2014). Entsiklopediya po zashchite ot virusov. Moskva.
11. Yakimenko, A. S. (2013). Sredstva zashchity informatsii. Moskva: Yuniti.
12. Mel'nikov, V. P. (2011). Zashchita informatsii v komp'yuternykh sistemakh. Moskva.

Göndərilib: 12.03.2024 Qəbul edilib: 15.05.2024