Azərbaycan Ali Texniki Məktəblərinin Xəbərləri
ISSN 1609-1620
Cild 22, № 5 (2020), 62-66
UOT 621.004.056

Korporativ idarələrdə informasiya təhlükəsizliyinin pozulması hallarının analizi

İnformatika və avtomatika

Həsənli X.F.
Azərbaycan Dövlət Neft və Sənaye Universiteti
E-mail: senan_jaf@rambler.ru

İnformasiya sistemlərinin təhlükəsizliyinin vacibliyi, fərd, idarə və təşkilatlar baxımından İT dünyasındakı imkanların sürətli inkişafına paralel olaraq artmaqdadır. İnformasiya sistemlərində təhlükəsizliyi təmin etmək üçün bir çox tədqiqatlar aparılıb və aparılmaqdadır. Aydındır ki, bu tədqiqatların aparılmasında məqsəd informasiya və informasiya sistemlərində təhlükəsizliyi yüksək səviyyədə təmin etməkdir. Bu məqsədlə istifadə olunan təhlükəsizlik proqramları fərd, idarə və təşkilatlara aid sistemlərin mühafizəsində böyük əhəmiyyət kəsb edir. Bu məqalədə geniş yayılmış təhlükəsizlik vasitələri ətraflı araşdırılır və 22 fərqli istifadə sahəsinə, funksionallığına görə kateqoriyalara bölünür. Bununla birlikdə fərd, idarə və təşkilatlar üçün informasiya sistemlərinin təhlükəsizliyinin təminə dair müxtəlif həllər çoxluğu sıralanıb. Beləliklə, mühafizə məsələlərində vacib əhəmiyyət kəsb edən möhkəm təhlükəsizlik siyasətləri, faydalı təhlükəsizlik vasitələri və müxtəlif muhafizə tədbirləri təqdim olunaraq fərd və ya təşkilati baxımdan lazım olan əsas təhlükəsizlik strategiyaları göstərilmişdir.

Açar sözlər: komputer mühafizəsi, informasiya təhlükəsizlik vasitələri, kiber hucumlar, cəsus proqramlar, məxfiliyin pozulması.

Giriş

İnformasiya sistemlərinin təhlükəsizliyinin vacibliyi fərd, idarə və təşkilatlar baxımından İT dünyasındakı imkanların sürətli inkişafına paralel olaraq olduqca aktual bir məsələdir və təhlükəsizliyi təmin etmək üçün müxtəlif texniki, texnoloji və təşkilati işlər görülsə də hələ də yüksək səviyyədə təhlükəsizliyi tam təmin etmək olmur.

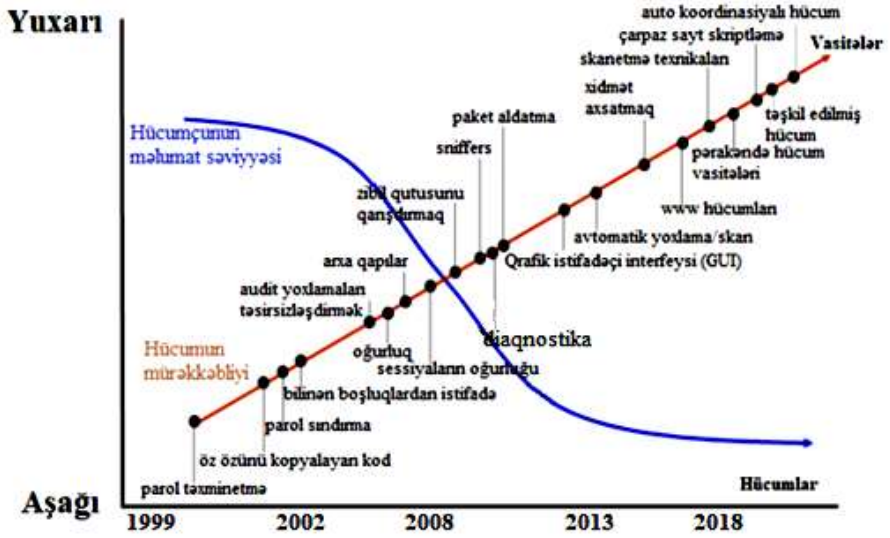
İnformasiya təhlükəsizliyi, informasiyanın icazəsiz girişlərdən, istifadəsindən, aşkar edilməsindən, silinməsindən, ziyan vurulmasından və ya dəyişdirilməsindən (tamlığının, izafiliyinin, konfidensiallığının pozulmasından) mühafizə metodudur. Təhlükəsizlik ümumiyyətlə bir haldır, vəziyyətdir – subyektin vəziyyətidir. İnformasiya mühafizəsi, komputer mühafizəsi və informasiya təhlükəsizliyi terminləri müxtəlif ədəbiyyatlarda bir-birinin əvəzinə istifadə edilib. Bu terminlər bir-biri ilə sıx əlaqəlidir, fərdi və ya təşkilati gizliliyin, bütünlüyün və informasiyanın əlyetənliyinin mühafizəsi məsələsində ortaq məqsədlərə sahibdirlər.

İnternetin çox geniş istifadə edilməsinə başlanmasıyla informasiya sistemlərindəki mühafizə və ya təhlükəsizlik boşluqları da artmağa başlamışdır. İnformasiya sistemlərindəki gizlilik, bütünlük və davamlılığın təmin edilməsi üçün bir çox muhafizə vasitələri və proyektlər inkişaf etdirilmişdir və hələ də inkişaf etməkdədir.

Məsələnin qoyuluşu

Komputer şəbəkə sistemlərindən geniş istifadənin başlanılmasıyla şəbəkə üzərindən edilən

hücumlarda (kiber hücumlar ing: cybrattack) artmışdır. Bu cür hücumların bir qisminə istifadəçilər istəmədən və ya bilməyərəkdən səbəb olurlar, digər qisminə isə bilərəkdən qəsdən zərər vermək istəyən bədniyyətli şəxslər səbəb olur. 1980-ci illərdə komputerlərarası rabitədə TCP/IP protokol ailəsi dünya səviyyəsində qəbul edilmiş və internet bu protokol vasitəsilə genişlənmişdir. İnternetin genişlənməsi ilə komputerlərarası əlaqədəki hücumların sayı və növü də artmışdır [1]. Bu hücumlar qarşısında identifikasiya, autoidendifikasiya, antivirus proqramları kimi müxtəlif mühafizə proqramlarından istifadə bir üst səviyyəyə keçmişdir və inkişafı daha da sürətlənmişdir. İlk əvvəllər hücumlar sadə kod əlavələri və ya parol təxminləri kimi daha sadə idi və təsiri də çox aşağı səviyyədə idi, lakin sonralar İT dünyasındakı sürətli inkişaf kiber hücumlarda da özünü göstərməyə başladı və hücumların təsiri daha çox zərərlərə, böyük maddi ziyanlara, vacib informasiya itkilərinə gətirib çıxardı [2]. Bu hücumları zərərsizləşdirə bilmək üçün bilik səviyyəsi aşağı idi. Çünki hücumlara səbəb olan informasiya internet üzərindən nəzarətsiz olaraq yayılırdı. Şəkil 1-də hücumların zamana görə intensivliyi, təsirləri və onları zərərsizləşdirə bilmək üçün lazımi bilik səviyyəsi göstərilmişdir.



Şəkil. 1. Hücumların zamana görə intensivliyi

İnformasiya təhlükəsizliyinə təhdidlər arasında təşkilat daxilində işləyən işçilərin yarada biləcəyi qərəzli və ya bilməyərəkdən təhdidlər olaraq müəyyən edə biləcəyimiz daxili təhdidlər çox vacib yer tutur. Qəsdən törədilən təhdidləri iki kategoriya üzrə sinifləşdirə bilərik, birinci kateqoriyaya idarədə çalışan bədniyyətli bir işçinin ona verilmiş sistemə giriş icazəsini şəxsi məqsədlərə istifadəsini, ikinci kateqoriyaya isə sıravi işçinin normalda özünün sistemə daxil olmaq üçün giriş icazəsinin olmadığı halda, başqa icazəsi olan birinə aid sistemə giriş məlumatlarını oğurlayaraq, sistemə qanunsuz yollarla daxil olaraq qorunan informasiyanı əldə edərək öz məqsədi üçün istədiyi kimi informasiyanı istifadə etməsini göstərə bilərik. Verilənlər bazasının administratorunun idarə elədiyi verilənləri şəxsi mənfəəti üçün başqa bir firmaya satmasının birinci kateqoriyaya misal kimi göstərə bilərik. Verilənlər bazasının administratoru olmadığı halda və normalda vb-yə giriş icazəsi olmayan bir işçi administratorun giris məlumatlarını oğurlayaraq sistemə giriş etməsini və şəxsi məqsədləri üçün vacib informasiya oğurlamasını isə ikinci kateqoriyaya aid misal kimi göstərə bilərik. *CSI (Computer Security Institute)* tərəfindən aparılan sorğunun nəticələrinə görə iştirakçıların 44 %-ı 2018-ci ildə daxili sui-istifadəyə məruz qalmışlar[5]. Bu nisbət daxili sui-istifadələrin 50 %-lik virus təhdidlərindən sonra ikinci ən böyük təhdid olduğunu göstərir. Bu cür sui-istifadələrin aşkarlanmasının çox çətin olduğunu və əksər bu cür sui istifadələrə məruz qalmış idarələrin öz nüfuzunu düşünərək bu barədə idarə xaricinə informasiya verilməməsinə diqqət göstərdiyini nəzərə alsaq əslində bu 44%-lik göstəricinin daha çox olduğunu düşünə bilərik.

Həll üsulları

İnformasiyaya daimi olaraq müraciətlərin təmin olunduğu mühitdə, informasiyanın serverdən müştəriyə qədər gizlilik içində, tamlığı pozulmadan, dəyişikliyə məruz qalmadan və kənar şəx-

slər tərəfindən ələ keçirilmədən tam mühafizə olunan şəraitdə çatdırılması müddəti informasiya təhlükəsizliyi olaraq müəyyənləşdirilir[6]. Təşkilati informasiya təhlükəsizliyi isə təşkilatların informasiya varlıqlarının təsbit edilərək zəifliklərinin müəyyən edilməsi və istənilməyən təhdid və təhlükələrdən qorunması məqsədilə lazımi təhlükəsizlik analizlərini apararaq tədbirlərin alınması kimi də düşünülə bilər.

Təşkilati informasiya təhlükəsizliyi insan faktoru, təhsil, texnologiya kimi bir çox faktorun təsir etdiyi tək bir damın altında idarə olunması məcburi olan qarışıq proseslərdən ibarətdir. Bu proseslərin idarə edilməsi, təhlükəsizlik sistemlərinin beynəlxalq standartlarda qurulması və yüksək səviyyədə informasiya təhlükəsizliyinin idarəsi altında standartlaşma işləri sürətlə davam edir. Standartlaşdırma məsələsində liderlik edən İngiltərə tərəfindən inkişaf etdirilmiş BS-7799 standartı, ISO tərəfindən qəbul edilmiş əvvəl ISO-17799, sonra isə ISO-27001:2005 adı ilə dünya səviyyəsində informasiya təhlükəsizliyi standartı olaraq qəbul edilmişdir[19].

Azərbaycan Respublikasında informasiya təhlükəsizliyi üzrə bir sıra qanunlar və normativ aktlar qəbul edilmişdir. Bu sahədə aşağıdakı qanunları göstərmək olar (siyahı bunlarla məhdudlanmır):

- İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Qanun;
- İnformasiya əldə etmək haqqında Qanun;
- Dövlət sirri haqqında Qanun;
- Fərdi məlumatlar haqqında Qanun;
- Kommersiya sirri haqqında Qanun;
- Elektron imza və elektron sənəd haqqında Qanun;
- Biometrik informasiya haqqında Qanun və s.

Nəqliyyat Rabitə və Yüksək Texnologiyalar Nazirliyində (NRYTN) fəaliyyət göstərən Standartlaşdırma üzrə "İnformasiya-kommunikasiya texnologiyaları" Texniki Komitəsi (TK 05) tərəfindən mövcud beynəlxalq standartlar əsasında bir sıra informasiya təhlükəsizliyi standartları işlənmişdir. Aşağıda onlardan bir neçəsi nümunə üçün verilir (tam siyahı ilə http://www.mincom.gov.az/ saytında *fəaliyyət-tənzimləmə-standartlaşdırma bölməsində* tanış olmaq olar):

- AZS 494-2010 (ISO/IEC 27001-2005) İnformasiya Təhlükəsizliyi. Təhlükəsizlik metodları. İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Tələblər;
- AZS 492-2010 (ISO/IEC 27005-2008) İnformasiya texnologiyaları – Təhlükəsizlik metodları – İnformasiya təhlükəsizliyi risklərinin idarə olunması;
- AZS 493-2010 (ISO/IEC TR 18044-2007) İnformasiya texnologiyası – Təhlükəsizliyin təmin edilməsinin metod və vasitələri – İnformasiya təhlükəsizliyi insidentlərinin idarə olunması" [7].

İdarə, təşkilat və müəssisələrin müəyyən təhlükəsizlik standartları çərçivəsində informasiya təhlükəsizliyini təmin edərək daxili və xarici təhdidlər qarşısında zərər görmədən və ya ən az zərərlə iş proseslərini davam etdirə bilmələri üçün informasiya təhlükəsizlik standartlarını öz təşkilatlarında tətbiq etmələri demək olar ki, zərurət halını almışdır.

Hazırda şəxsi şirkətlər və dövlət müəssisələri işlərini davam etdirmələri üçün intensiv şəkildə informasiya istifadəsinə yönəlmişlər. Zaman keçdikcə informasiyanın əhəmiyyəti artmış, sadəcə təhlükəsiz bir şəkildə saxlanması və arxivlənməsi tələblərə cavab verə bilməyib eyni zamanda bir yerdən başqa bir yerə transfer edilməsi danılmaz bir ehtiyac halına çevrilmişdir. İnformasiyaya olan bu asılılıq informasiyanın qorunmasını və mühafizəsini gündəmə gətirmişdir. Bu mənada informasiya təşkilatın sahib olduğu varlıqlar arasında çox əhəmiyyətli yerə sahibdir.

İnformasiya müəssisədəki digər varlıqlar kimi müəssisə üçün əhəmiyyət kəsb edən və bu səbəblə də ən yaxşı şəkildə qorunması vacib olan bir varlıqdır. İnformasiyanın bir çox şəkildə istifadəsi göstərilə bilər. İnformasiya kağız üzərində yazılı şəkildə ola bilər, elektron versiyada saxlanıla bilər, e-poçt vasitəsilə bir yerdən başqa bir yerə transfer edilə bilər və ya şəxslər arasında sözlü olaraq ifadə edilə bilər. İnformasiya hansı formada olursa-olsun mütləq uyğun bir şəkildə mühafizə olunmalıdır.

İnformasiya təhlükəsizliyi əsasən aşağıdakı üç elementə hədəflənib:

- Gizlilik (Confidentiality);
- Bütünlük (Integrity);
- İstifadə imkanları - əlyetənlik (Availability).

Nəticə

Bu anlayışlar aydınlaşdırılaraq gizlilik, informasiyanın icazəsiz müdaxilələrdən qorunması kimi müəyyənləşdirilir. Gizlilik – informasiyanı icazəsi olmayan şəsxlər tərəfindən aşkarlanmasının qarşısını almaqdır. Bütünlük – informasiyanın icazəsiz şəxslər tərəfindən dəyişdirilməsi, silinməsi və ya hər hansı bir şəkildə təhrif edilməsi təhdidlərinə qarşı məzmununun qorunmasıdır. Bütünlük üçün qısaca bilməyərəkdən və ya qəsdən informasiyanın pozulmaması deyə bilərik. İstifadə imkanları, yəni əlyetənlik – informasiyanın ona ehtiyac olduğunda istifadəyə hazır vəziyyətdə olması deməkdir. Hər hansı bir problem yaranan zaman belə informasiyanın əlyetən olması istifadə imkanı baxımından vacib bir xüsusiyyətdir. Bu imkan istifadəçinin hüquqları çərçivəsində olmalıdır. Əlyetənlik ehtiyac prinsipi baxımından hər istifadəçinin giriş icazəsinin olduğu informasiya mənbəyinə, səlahiyyət müddətində mütləq istifadə edə bilməsi əsaslandırılmışdır.

Ədəbiyyat

1. DeNardis L. The History of Information Security. // A coprehensive handbook. – Elsevier, 2007.

2. Brendan P. Kehoe, Zen and Art of the Internet, http://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html# SEC91 , 1992,CERT Advisory CA-90:01, Sun sendmail vulnerability, January 29 (1990).

3. https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/secure-infrastructure/net_implementation_white_paper0900aecd803fcbbe.pdf.

4. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. – Bakı: İnformasiya Texnologiyaları, 2012. – 219 səh.

5. http://jpis.az/uploads/article/az/2018_2/ENTROPY_WEIGHTS_AND_DYNAMIC_INDEX_FOR_NATIONAL_CYBERSECURITY.pdf.

6. https://www.cbar.az/assets/2482/Informasiya_texnologiyalari_standarti.pdf.

7. Kalman S. Web Security Field Guide. – Cisco Press, Indianapolis, 2003. – P.36, 37.

Резюме

Гасанли Х.Ф.

Анализ нарушений информационной безопасности в корпоративных офисах

Важность безопасности информационных систем возрастает параллельно с выдающимися достижениями в мире информационных технологий с точки зрения отдельных лиц, управлений и организаций. Многие исследования были проведены с целью обеспечения безопасности информационных систем. Целью этих исследований является обеспечение безопасности информации и всей информационной системы на высшем уровне. Для этой цели используемое защитное программное обеспечение очень важно для защиты систем принадлежащих лицу, учреждению или организациям. В этой статье были подробно рассмотрены широко используемые средства безопасности, которые в зависимости от области применения и функционирования были классифицированы по 22 категориям. В то же время перечислены различные методы решения для обеспечения безопасности информационных систем для лиц, учреждений и организаций. Таким образом, рассматривая мощную политику безопасности, имеющую огромное значение при решении проблемы защиты, а также другие полезные средства и меры защиты, были показаны основные стратегии безопасности, необходимые для отдельных лиц или организыций.

Ключевые слова: компьютерная безопасность, средства защиты информации, кибератака, шпионская программа, нарушение конфиденциальности.

Summary
Hesenli Kh.F.
Analysis of information security breaches in corporate offices

The importance of the security of information systems has been increasing for person, institution, and organizations in parallel to extraordinary advancements in the IT world. Many studies have been done in order to provide security for information systems. The purpose of these studies is to provide security in information and informatics system. For this purpose, used security software is very important to protect the systems belong to person, institution or organizations. In this paper, prevalently used security tools were examined in detail and these tools were categorized according to functionality, usage area as 22 categories. At the same time, various solutions are listed to ensure the security of information systems for person, institution and organizations. So, constructive security policies that are important for safety information system and other useful means and measures of protection presented for fundamental of security strategies are needed for personal or institutional factors.

Key words: computer security, information security tools, cyberattacks, spyware, confidentiality breach.