UOT 004.056

Yunusov T.E
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
turaly@mail.ru

KOMPÜTER SİSTEMLƏRİ TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ XÜSUSİYYƏTLƏRİ

Məqalədə kompüter sistemlərinin təhlükəsizliyinə olan təhdidlər, texniki vasitələrin zəifliklər, qərəzli yaradılan proqram səhvləri,hücumlar üçün istifadə olunan üsullar, insan faktoru kimi zəifliklər analiz edilmişdir. Həmçinin təhlükəsizliyin qiymətləndirilməsi üçün taksonomiyalar və onların xüsusiyyətləri analiz edilmişdir.

Açar sözlər: *kompüter sistemləri, təhlükəsizliyin qiymətləndirilməsi, təhlükələrin analizi, təhlükəsizliyin qiymətləndirilməsi taksonomiyaları, taksonomiyaların xüsusiyyətləri.*

Giriş

Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi mürəkkəb problemdir. Təhlükəsizliyin qiymətləndirilməsində göstərilən son səylərin əksəriyyəti mühafizə sistemində olan zəifliklərin aşkarlanmasını nəzərdə tutur. Mühafizə sistemində olan naməlum zəifliklərin aşkar edilməsi hələ də subyektiv prosedur olaraq qalmaqdadır. Prosedur, tanınmış mühafizə sistemində olan zəifliklərin xüsusiyyətlərini nəzərə almaqla necə təkmilləşəcəyini bilir. Buna görə, əldə olunmuş məlumatlar müvafiq təsnifata daxil edilir, daha sonra mühafizə sistemində naməlum olan zəifliklərlə əlaqəli olaraq, yeni sistemlərin araşdırılması üçün sistematik struktur kimi istifadə olunur. Belə təsnifatların işlənməsində bir sıra cəhdlər olmuşdur. Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi, sistemin hücumlara qarşı müqavimət göstərmə bacarığının təyin edilməsi prosesidir. Bu proses, tipik olaraq, məlum zəifliklərin aşkarlanması üçün sistemdə edilən yoxlamaları nəzərdə tutur, çünki hücumların çoxunda kompüter sistemlərindəki məlum zəifliklərdən istifadə edilir. Mühafizə sistemindəki zəifliklər hücumçuya sistemin informasiya əminliyini azaltmaq imkanı verir.

Kompüter sistemlərinə olan təhlükələrin analizi

Kompüter sistemlərinin təhlükəsizliyinə olan təhdidlər üç əsasın birləşməsidir – sistem zəifliklərı, hücumçunun səhvlərdən istifadə etməsi və məqsədinə çatmaq üçün sistemdəki səhvlərdən istifadə edərək xüsusi alətlərlə sistemdən faydalanmaq bacarığı [1]. Zəyiflikdən istifadə etmək üçün, hücumçu ən azı elə bir alət və ya üsullara malik olmalıdır ki, həmin alətlərin vasitəsilə sistemin hər hansı bir zəif nöqtəsinə qoşula bilsin. Bu çərçivədə, zəifliyin aşkarlanması hücumun ilkin mərhələsi kimi də tanınır. Zəifliklərin idarə edilməsi zəifliklərin tanınmasının, təşkilinin, düzəliş edilməsinin və azaldılmasının müntəzəm şəkildə yerinə yetirilməsidir. Ümumiyyətlə, belə bir idarəetmə hesablama sistemlərində olan proqram zəifliklərinə əsaslanır. Təhlükəsizlik ehtimalı zəiflik kimi təsnif edilə bilər. Təhlükə, əhəmiyyətli bir uğursuzluğun ehtimalı ilə bağlıdır. Deməli, heç bir təhlükəyə malik olmayan zəifliklər də mövcuddur [2].

İş fəaliyyəti nəticəsində yaranan boşluqlar və ya tamamilə yerinə yetirilmiş hücumlar istifadəyə yararlı olan zəifliklər kimi təsnif edilirlər. Proqram təminatında təhlükəsizlik boşluğu aşkarlanan zaman giriş ləğv edilir, təhlükəsiz qoşulma üçün başqa üsullar təklif edilir və ya hücum dayandırılır.

Proqram təminatına bağlı olmayan zəifliklər də mövcuddur. Texniki vasitələrdə, proqram təminatında təhlükəsizlik boşluqları olmayan sistemlərdə insan faktorunu nümunə kimi göstərmək olar [3]. Müvafiq şəkildə istifadəsi çətin olan proqramlaşdırma dillərində konstruksiyalar boşluqların böyük mənbəyi ola bilərlər. Bildiyimiz kimi, boşluqlar kompüter sisteminin zəif nöqtələridir, məsələn onlar prosedurlarda, planlarda ola bilər və ya tətbiq zamanı yanılma

nəticəsində baş verə bilər və zərər vermək məqsədilə istifadə oluna bilərlər. Aşağıda ümumi zəifliklərdən bir neçəsi gostərilmişdir:

Texniki vasitələrin zəifliklərı – aparatın sıradan çıxarılması: daxil edilmiş aparaturaya ciddi zərər vurulması təsadüf deyil. Aparatdan asılı olan qırılma adətən həqiqətdə kompüter aparatına və proqram təminatına zərər vurmaq istəyənləri nəzərdə tutur.

Proqram təminatı zəifliklərı – kompüter sistemlərinin təhlükəsizliyinə olan təhlükələrin böyük bir qismi proqram təminatı zəifliklərinin nəticəsidir. Bu zəyifliklərdən istifadə edərək bədəməl sistem prosesini dayandıra, gedişatı pozub istədiyi kimi proqramlaşdıra və ya informasiya oğurlaya bilər.

Sistemi dəyişdirən və ya sistemi pozan proqramlar aşağıdakılardır:

Məntiqi bombalar: kiçik proqramlardır, hansı ki, verilmiş şərait və ya verilmiş vaxt proqramla uyğunlaşdıqda, proqram aktivləşir, istənilən komandanı yerinə yetirə bilir.

Troyan: casus proqramlar, əsas funksiyalarından biri sistemdə olan informasiyanı proqramçıya ötürməkdir.

Virus proqramlar: müxtəlif vasitələrlə bir kompüterdən digər kompüterə keçməyə cəhd edən, verilənlərin korlanmasına, dəyişdirilməsi və silinməsinə gətirən və ya istifadəçinin işinə mane olan, digər proqramlarda gizlənmiş kiçik həcmli proqramlardır:

- *Trapdoor* – gizli çıxış nöqtəsi olan proqram;
- *Information leaks* – informasiyanı proqramlarla sızdıran xüsusi kodlar;
- *Theft* – proqramların və lisenziyaların qanunsuz köçürülməsi üçün proqramlar.

Qərəzli yaradılan proqram səhvləri:

Yaddaş daşmaları – kompüter proqramı tərəfindən verilənlərin bufer yaddaşındakı seçilmişlərdən kənarda yazılması fenomeni adlanır.

Natamam vasitəçilər – sistem istifadəsi zamanı yaranan səhvlər.

Yoxlama zamanı yaranan səhvlər – istifadə olunan proqramlarda edilmiş dəyişikliklərin proqram tərəfindən yoxlanması zamanı yaranan səhvlər.

Hücumlar üçün istifadə olunan üsullar:

- *Konfidensiallıq səhvləri*. Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur. Protokolların qüsurları, hərəkətləri izləmə, passiv əlaqənin dinlənməsi, çatdırılma itkiləri və traffkin analizi hücumlar üçün istifadə olunan konfidensiallıq səhvləridir.
- *Bütövlük qüsurları*. Bütövlük informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər. Aktiv əlaqənin dinlənməsi, təqlid, mesajın saxtalaşdırılması, küy, web səhifələrin silinməsi və DNS hücumları bütövlük qüsurlarıdır.
- *Əlyetənlik səhvlər*. Əlyetənlik yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda, uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır [4]. Kommunikasiya və ya modul səhvləri, xidmətdən imtina, DNS hücumlar, trafikin yönləndirilməsi və DDOS hücumları əlyetənlik səhvləridir.

- *Kəşfiyyat*. Sistemdə aparılan ümumi səhvlərin və boşluqların axtarışı prosesidir. Portların axtarışı, sosial mühəndislik, əməliyyat sistemlərində və proqramlarda qoyulan izlər hücumlar üçün istifadə olunan kəşfiyyat prosesidir.
- *Autentifikasiya səhvləri*. Sistemə giriş üçün istifadə edilən uğursuzluqlardır. Təqlid etmə, təxmin etmə, hərəkətləri izləmə, spufinq və sesiyanın ələ keçirilməsi hücum üçün istifadə olunan üsullardır.
- *İnsan faktoru*. Kompüter sistemlərinin təhlükəsizliyinin təmin edilməsində insan faktoru əsas rol oynayır və vacib zəif nöqtələrdən biri ola bilər. Tələbkar, narazı bir şirkət əməkdaşı sistem məlumatlarını və faktlarını daxildən zədələyə bilər. Həmçinin təşkilata ziyan vurmaq istəyən və ya orada olan informasiyanı oğurlamaq istəyən kənar şəxs təşkilat işçilərini müəyyən məbləğlə satın alaraq öz istəklərinə nail ola bilirlər.

Taksonomiyalar və təhlükəsizliyin qiymətləndirilməsi

Taksonomiya "elmi təsnifatın ümumi prinsiplərinin öyrənilməsi" kimi təsvir olunur [5]. Taksonomiya sözü, bundan əlavə, obyektlərin faktiki olaraq kateqoriyalarını göstərmək üçün də istifadə olunur. Bu təsnifat, obyektlərin fərqləri arasında olan birləşmələrə əsasən tamamlanır. Eyni zamanda real sahədə elmi tədqiqatın başlanması zamanı, yüksək keyfiyyətli taksonomiya "sistemli iş üçün əhəmiyyətli və əsas tələb" kimi ölçülür [6]. Sistematik araşdırma üçün böyük miqdarda informasiyanın obyektlərdən səysiz toplanılması çox da konstruktiv deyil.

Bundan başqa, taksonomiya mövzunun öyrənilməsi üçün ümumi dil təklif edir. Əvvəldə tövsiyə edildiyi kimi, zəifliklərin taksonomiyası təhlükəsizlik dərəcəsinin qiymətləndirmə prosedurunda faydalı ola bilər. Həmçinin, zəifliklərin və hücumların taksonomiyası sistem layihəçisi üçün faydalı ola bilər. Layihəçilərə kömək edə biləcək informasiyalar struktur xüsusiyyətlərini pozmamalıdır. Zəifliklərin taksonomiyası, bundan başqa, naməlum hücumları aşkar etmək üçün üsul təklif edir. Zəif bənd və ya taksonomiyada altbölmə istifadə potensialını xarakterizə edir. Əgər taksonomiyanın ciddiliyinə inanıb müvafiq olaraq zəifliklər seçə bilən pillə sistemi kimi qəbul etsək, müdafiə qrupunun aktivlərini üstün tutacaq yeni sistem yaratmış olarıq. Ən son zəifliklər və hücumlar haqqında informasiyanın yayılmasına kömək etmək məqsədilə, bir sıra təhlükəsizlik təşkilatları zəifliklər əsaslı araşdıran baza saxlayırlar. Misal üçün, US-CERT (United States Computer Emergency Readiness Team) məlumat bazası və ümumi zəifliklərin və mühafizə üsullarının məlumat bazasıdır. Ən son zəifliklər aşkar edən təşkilatlar və ya hər hansı bir tərəf, bu məlumatı mərkəzə göndərir və burada həmin zəifliklər təsnif edilir və toplanılır [7].

Bundan başqa, taksonomiya CERT (Computer Emergency Response Team) kimi komandalara cavab vermək məqsədilə müdafiə üçün məntiqli bir dil təklif edir. Zəifliklərin və hücumların çoxsaylı taksonomiyaları illər boyu mövcud idi, amma indiyədək hər hansı bir standartla müəyyən edilmiş taksonomiya mövcud deyildi. Bir sıra fərqli taksonomiyalar mövcuddur və onların hər biri dəqiq sahələrə uyğundur. Tanınmış zəifliklər və hücumlar əsasında təhlükəsizlik qiymətləndirmə prosedurunu qurmaq mümkündür lakin tanınmamış zəifliklər və hücumların təyini üçün üsulun seçilməsi çətindir. Bu prosesin analizi taksonomiyaların növlərini, nöqsanlarını və üstünlüklərini aşkar etməyə imkan verir [8, 9]. Təhlükəsizlyin qiymətləndirilməsi ilə bağlı olan aspektlərin müəyyən edilməsi uzun vaxt aparır.

Təhlükəsizliyin qiymətləndirilməsi üçün taksonomiyaların xüsusiyyətləri

Kompüter təhlükəsizliyində taksonomiyaların məqsədi müxtəlif hücumları və zəifliklərı təklif edərək və nəzərə alaraq sistemi ifadə etməkdən ibarət idi. Təhlükəsizlik qiymətləndirmə prosedurundan səmərəli surətdə necə istifadə onlunmasını bilən şəxs taksonomiyaları istifadə etdiyi sistemə uyğunlaşdırmalıdır. Bundan başqa, bu prosedurun qısaca və dəqiq, həm obyektiv, həm də müəssər ifadə edilməsinə kömək etməlidir. Hücumlar üçün istifadə olunan sistem zəifliklərı aradan qaldırılmalı və hücumların qarşısı alınmalıdır. Hücumları taksonomiyalar üzrə

kateqoriyaya bölsək, əsas ölçülər: təsir, hədəf, mənbə və zəiflik olar. Zəifliklərdən başqa, təsir, hədəf və mənbə növlərinin sayı verilmiş sistem üçün məhduddur. Zəifliklərin sayı həmişə naməlumdur və təhlükəsizlik qiymətləndirmə prosedurunun məqsədi onların aşkar edilməsindən ibarətdir. Deməli, hücumlar haqqında informasiya təşkilinin texniki üsulları, hücumun nəticəsindən başlayaraq tədricən zəifliklərin aşkar edilməsinə doğru hərəkət edərək, iyerarxik şəkildə olacaqlar. Tələb edilən sistem üçün inkişaf etdirilmiş taksonomiyalar nadir hallarda digər sistemlər üçün yararlıdır. Bu isə ədəbiyyatda taksonomiyaların çox olmasının səbəblərindən biridir. Onların hər biri sistemin dəqiq tipinə yönəlmiş olur. Taksonomiya iyerarxik olmalıdır və iyerarxik taksonomiya zəiflikləri tanımaq üçün məqsədli metodologiya təklif edir. Müqayisə üçün , xətti və ya horizontal taksonomiyalar sadəcə hücumun xüsusiyyətlərini nəzərə almaq üçün faydalıdır. Həmin informasiyanın istifadəsi isə onun üzərində qiymətləndirməni yerinə yetirən şəxsdən asılı olardı. Taksonomiya hesab edilən təhlükənin yüksək intensivliyindən başlanmalıdır və tədricən aşağı enməlidir. Hələ də, çox miqdarda təqdim edilmiş taksonomiyaların ən aşağı səviyyəsi, hücumun və ya zəifliyin yüksək səviyyəli illüstrasiyasına malikdir.

Hücumlar üçün taksonomiyanın aşağıdakı klassifikasiya səviyyələri mövcuddur.

Birinci səviyyə – hücum təsiri: bütün hücumlar təhlükəsizlik boşluğunun xüsusiyyətlərindən istifadə edirlər. Beləliklə, hər hücum pozduğu təhlükəsizlik xüsusiyyətləri altında qruplaşdırıla bilər. Hücumçu bir dəfə təhlükəsizlik siyasətini pozduğu təqdirdə, o bir sıra hücumları yerinə yetirə bilər. İkinci dərəcəli hücumlar sadəcə olaraq hücum edənin istəyindən asılıdır.

İkinci səviyyə – müəyyən hücumların tipləri: buna misal olaraq DOS hücumlarını və DDoS hücumlarını göstərmək olar. DoS–hücum (ing. Denial of Service − xidmətdən imtina) veb saytın, veb serverin və digər şəbəkə resursunun normal işini pozmaq və ya çətinləşdirmək məqsədilə həyata keçirilir. Bu hücumları müxtəlif üsullarla həyata keçirirlər. Üsullardan biri serverə çoxsaylı sorğuların göndərilməsidir, serverin resursları onların emalı üçün yetərli olmadıqda, serverin işi çətinləşə və ya pozula bilər. DDoS (Distributed Denial of Service − paylanmış xidmətdən imtina) hücumunda şəbəkə resurslarına bir deyil, çox sayda kompüterdən sorğular göndərilir. Yoluxdurulmuş kompüterlərdən biri "idarəetmə mərkəzi" kimi istifadə edilir, o "zombi" adlandırılan digər kompüterlərdən edilən hücumları idarə edir [10].

Hər bir sistem hücumların spesifik tiplərinin kiçik sayına məruz qalır. Hücumun ani effekti bəzi təhlükəsizlik xüsusiyyətlərinin müvəffəqiyyətsizliyidir [11].

Üçüncü səviyyə – sistem komponentlərinə olan hücumların hədəfidir: butün hücumlar sistemin altsistemlərini hədəf seçir. Hərtərəfli, ardıcıl qiymətləndirməni yerinə yetirmək üçün bütün sistem mexanizmlərinə baxılmalıdır. Məsələn, əgər protokolun zəifliklərini qiymətləndirsək, klasifikasiyanın üçüncü səviyyəsi burada protokol səviyyələrinin müxtəlifliyi olacaqdır. Belə bir klasifikasiyanın illustrasiyası burada əməliyyat sistemində DoS hücumlarının ehtimalını araşdırır.

Dördüncü səviyyə – sistemin xüsusiyyətlərində olan zəifliklərin mənbələrinə baxılır. Təhlükəsizlik qiymətləndirmə prosedurasının effektivliyi onun müstəqilliyi və zəifliyin emalı ilə qiymətləndirilir. Əgər zəifliklərin qiymətləndirilməsi üçün metrikalar olmazsa, yuxarıda göstərilmiş xüsusiyyətləri olan taksonomiya çox böyük təhlükəizlik qiymətləndirmə prosedurunda köməkçi rol oynayacaqdır.

Nəticə

Kompüter sistemləri günü-gündən inkişaf edir və həyatımızın hər bir sahəsində tətbiq olunur. Kompüter sistemlərinin tətbiqi və istifadə sahələri genişləndikcə, ona olan təhlükələrin və hücumların sayı artır. Belə məsələlərə hazırlıqlı olmaq üçün kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi metod və taksonomiyalarından istifadə edilir.

Təhlükəsizliyin qiymətləndirilməsi mürəkkəb bir problemdir, hücumların və zəifliklərin taksonomiyası bu problemin həlli üçün istifadə oluna bilər. Bu tədqiqat kompüter və şəbəkə təhlükəsizliyinə aid olan bütün taksonomiyaların ümumi xüsusiyyətlərini göstərmişdir. Məqalədə

təhlükəsizliyin taksonomiyası üzrə təqdim edilmiş işlər tədqiq edilir və təhlükəsizliyin qiymətləndirilməsi üsullarının effektivliyi qiymətləndirilir.

Ədəbiyyat

1. The Three Tenents of Cyber Security. U.S. Air Force Software Protection Initiative. http://www.spi.dod.mil/tenets.htm. Retrieved 2009–12–15.
2. Foreman. P: Vulnerability Management, page 1. Taylor & Francis Group, 2010. ISBN 978–1–4398–01505.
3. J. D. Howard and T. A. Long staff. A Common Language for Computer Security Incidents, Sandia tech.rep. SAND98–8667, Oct. 1998.
4. U.Lindquist and E. Jonsson. How to Systematically Classify Computer Security Intrusions, Proc. IEEE Symp. Sec. and Privacy, 1997, 4–7 May, pp.154–63.
5. C. E. Landwehr et al. A Taxonomy of Computer Program Security Flaws, ACM Comp. Surveys, 1994, vol.26, no.3, Sept. pp.211–54.
6. J. Mirkovic and P. Reiher. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Comp. Commun. Rev., 2004, vol.34, no.2, pp.39–53.
7. CERT Coordination Center Vulnerability Database, http://www.kb.cert.org/vuls .
8. Common Vulnerabilities and Exposures List, http://www.cve.mitre.org/ .
9. M. Bishop. Vulnerabilities Analysis, Proc. 2nd Int'l. Symp Recent Advances in Intrusion Detection, Sept. 1999, pp.125–36.
10. V. Raskin et al. Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool, Proc. NewSec. Paradigms Wksp., Cloudcroft, NM, 2001, pp.53–59.
11. Gray. An Historical Perspective of Software Vulnerability Management, Info. Sec. Tech. Rep., 2003, vol.8, no.4, pp.34–44.

УДК: 004.056

Турал Юнусов Е.
Институт Информационных Технологий НАНА, Баку, Азербайджан
turaly@mail.ru

Особенности оценки безопасности компьютерных систем

В статье проанализированы угрозы безопасности компьютерных систем, уязвимости технических средств, ошибки вредоносных программ, методы, используемые для атак, уязвимости, связанные с человеческим фактором. Также были проанализированы таксономии оценки безопасности компьютерных систем и их характеристики.

Ключевые слова: *компьютерные системы, оценка безопасности, анализ угроз, таксономия оценки безопасности, особенности таксономии.*

Tural E. Yunusov
Institute of Information Technology of ANAS, Baku, Azerbaijan
turaly@mail.ru

Features of computer system security assessment

The article analyzes the threats to security of computer systems, hardware vulnerabilities, malware error, the methods used for attacks, vulnerabilities related to human factor. Also taxonomy of computer systems security evaluation and their characteristics analysis have been conducted.

Key words*: computer systems, security assessment, threat analysis, security assessment taxonomies, taxonomies features.*