Kompüter sistemlərində informasiya təhlükəsizliyi auditinin aparılması üsulları

Tural Yunusov

AMEA İnformasiya Texnologiyaları İnstitutu
turaly@mail.ru

***Xülasə*— Məqalə kompüter sistemlərində informasiya təhlükəsizliyi auditinin aparılması üsullarına həsr edilmişdir. Məqalədə kompüter sistemlərinin təhlükəsizliyi auditinin bəzi standart və metodları, o cümlədən İSO 27000, kompüter sistemlərində təhlükəsizlik riskləri, kompüter sistemləri təhlükəsizliyi üçün auditin planlaşdırılması analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin mövcud təhlükəsizlik audit metodları nümunə göstərilmişdir.**

Açar sözləri— kompüter sistemləri; təhlükəsizliyin auditi; informasiya təhlükəsizliyi auditi; təhlükəsizlik riskləri; audit standartları; audit üsulları.

I. GİRİŞ

Bugünki gündə kompüter sistemləri həyatımızın hər bir sahəsində aktiv rol oynayır. Bu sistemlərdə şəxsidən təşkilata qədər, vacib olmayandan ən vacib informasiyaya qədər çox geniş növ verilənlər saxlanılmaqda və istifadə olumaqdadır.

Həm bu qədər məlumatları saxlaması həm də informasiya texnologiyalarının iş və şəxsi həyatdakı rolunun ciddi bir şəkildə artmasıyla əlaqədar kompüter sistemlərinin təhlükəsizliyi çox vacib əhəmiyyət qazanmışdır. Kompüter sistemlərində lazımlı təhlükəsizlik tədbirlərinin alınmaması bu sistemlərdən məlumatların oğurlanmasını, məlumatın təxribatı və məhv edilməsinə qədər fərqli nəticələr yarada bilər. Buradakı təxribatın təsiri oğurlanan məlumatın vacibliyi ilə düz mütənasib olaraq artır və bəzən bərpa olunmaz zərərlər verə bilməkdədir.

Bu cür bərpa olunmaz zərərlərin qarşısını almaq üçün və sistemlərin etibarlı bir şəkildə işini təmin etmək üçün kompüter sistemlərində informasiya təhlükəsizliyi auditinin aparılması vacibdir. Təhlükəsizlik auditi müəyyən müddətlərdə tekrarlanmalı və sistemlərdə aşkar edilən zəifliklər ən qısa vaxtda bağlanılmalıdır.

Kompüter sistemləri üçün təhlükəsizlik auditi ilə əlaqədar çoxlu mənbə vardır. Bu mənbələrin arasında ən çox istifadə olunanlar audit edilən sistemlər üzərindəki tətbiqləri təmin edən istehsalçı firmalar gəlməkdədir. Məsələn; Microsoft sistemləri üçün TechNet və ya Microsoftun dəstək səhifəsinə müraciət edilə bilər. Bu mənbələrlə yanaşı təhlükəsizlik auditi ilə əlaqədar təhlükəsizlik sahəsində ixtisaslaşmış müxtəlif təşkilatların hazırladığı materiallardan da faydalanmaq olar. Bu mərhələdə SANS və CIS təşkilatlarının əməliyyat sistemi, verilənlər bazası sistemləri, veb tətbiqləri və s. mövzuları haqqında və fərqli məhsullar ilə əlaqədar sənədləri də istifadə etmək olar.

II. TƏHLÜKƏSİZLİK RİSKLƏRİ

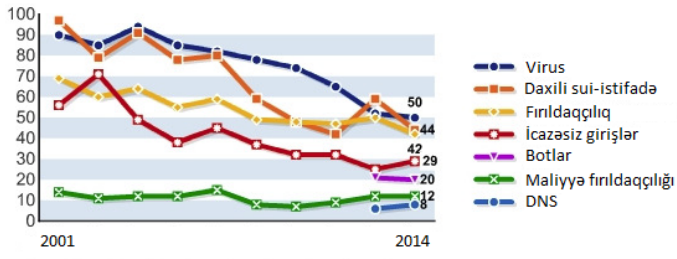
Kompüter sistemlərinin qorunmalı olduğu iki risk qrupu vardır: Fiziki risklər və məntiqi risklər. Fiziki risklər daha çox avadanlıq hesabına meydana gəlirlər, hansı ki, bura təbii fəlakətlər -zəlzələ, qasırğa, tornado, sel daxildir, əlbəttə başqa təhlükələr də mövcuddur, partlayış, yanğın, oğurluq, icazəsiz müdaxilələr kimi. Champlain-də fiziki təhditlərin idarə edilməsi və müəyyənləşdirilməsi üçün siyahı mövcuddur [1].

Bu nəzarət tədbirləri aşağıdakılardır: kilidləmə növləri, avadanlıq sığortası və yeniləmə xərcləri, kompüter sistemlərinin və məlumatların günlük arxivləşdirmə üçün icra prosedurları, məlumatın və arxivlərin təhlükəsiz yerdə saxlanılması və yoxlanılmış yenidən bərpa sistemi.

Məntiqi risklərə informasiya sisteminin və məlumatlarınıın təsadüfi, qəsdən məhv edilməsi və ya dəyişdirilməsi aiddir. Bu təhdidlər qarşısını sistem istifadəçilərinin giriş imkanlarını məhdudlaşdıraraq və sistemə icazəsiz girişlərin sayı məntiqi idarə etmə ilə azaldıla bilər. Bütün bu tədbirlər kritik kompüter sistemləri üçün çox vacibdir.

Symantec-ə görə İT riskləri 4 əsas növü vardır: Təhlükəsizlik riskləri, mövcud risklər, performans riskləri, uyğunluq riskləri [2]. Təhlükəsizlik risklərinə informasiyanın oğurlanması, icazəsiz girişlər, məlumatın bütövlüyü, elektron fırıldaqçılıq aiddir. Təhlükəsizlik risklərinə həmçinin xarici təhdidlər, viruslar kimi, hədəfli xüsusi proqramlarla edilən hücumlar, xüsusi istifadəçilər və xüsusi informasiyalar daxildir. "Ernst and Young" sorğusu göstərdi ki, təhlükəsizlik hadisələri şirkətlərə 17-28 milyon dollar ziyan verib [3] [4]. Başqa bir sorğu 13 il ərzində Amerikada baş vermiş təhlükəsizlik hadisələrini 522 komputer vasitəsi ilə statistika hazırlamışdır [5]. Nəticələrə əsasən virusla bağlı hadisələr ən çox olub 49% təşkil edir. İkinci ən çox olan daxildən şəbəkəyə təhdidlər 44% təşkil edir, ardınca laptop və mobil cihazlarla bağlı hadisələr 42% yer alır. Şəkil 1-də təhdidlərin növləri göstərilmişdir.

Lampson qeyd edir ki, obyektin giriş matris modeli, icazələri idarə olunması siyahısı, açıq açarla kriptoqrafiya və kriptoqrafik protokollar kimi informasiya təhlükəsizliyi sahəsində mühüm nailiyyətlərə baxmayaraq çox kompüter sistemləri daxilində və ya xaricində hücumlara məruz qalırlar [6]. Təhlükəsizliyin qurulması vaxt aparır, ancaq effektivliyi yalnız audit və hücum vaxtı müəyyən edilir.



Şəkil 1: Təhdidlərin növləri

Kompüter fəaliyyətinin üç istiqaməti müntəzəm olaraq nəzarət olunmalıdır: istifadəçi icazələrinin idarə olunması, sistem fəaliyyətinin monitorinqi və audit. Bu fəaliyyətlər təhlükəsizliyin həyata keçirilməsi üçün əsas mexanizmlərdir [6]. a) *autentifikasiya* prinsipləri ("Kim dedi?" və ya "Bu informasiyanı kim əldə etdi" – insanlar, qruplar, maşınlar və ya proqramlar); b) *səlahiyyət* icazələri ("Bu əməliyyatı etmək üçün kim inamlıdır?"); c) *audit* aparılması ("Nə baş verib və nə vaxt?").

İstifadəçi icazələrinin idarə olunması sahəsində təhlükəsizliyin məqsədi, səhvləri və fırıldaqçılıq riskini azaltmaq, icazəsiz girişlərin aradan qaldırılması və məlumatların məxfiliyini təmin etməkdir. Sistem fəaliyyətinin monitorinqi çox vacib faktordur, çünki təxribat və fırıldaqçılıq hadisələrinin baş verməsi çox yüksəkdir.

Risk olan sahədə dörd sual soruşulmalıdır: 1) Bu burada ola bilər? 2) Necə? 3) Təhlükəsizlik tədbirləri təhdidləri aşkarlamaq üçün kifayət edirmi? 4) Tədbirləri necə inkişaf etdirə bilərik? [7]. Effektiv sistem təhlükəsizliyi və idarə etmə proseduraları hadisələrin qarşısının alınması və təhdidlərin aşkarlanması risk səviyyəsini azaltmaqdadır.

Digər vacib təhlükəsizlik tədbiri isə detallı loqların saxlanılmasıdır, hansıki burada, kim və nə vaxt etdi və ya təhlükəsizlik pozuntusu varmı kimi suallara cavab tapmaq mümkündür.

III. AUDİT STANDARTLARI

ISO/IEC 18028-3 əsasən, İT şəbəkə təhlükəsizliyi – 3-cü hissə: Təhlükəsiz şəbəkə keçidləri istifadə edən şəbəkələr arasında təhlükəsizlik əlaqələri, audit "rəsmi sorğu, rəsmi araşdırma və ya gözləninlərə qarşı faktların yoxlanmasıdır." [8].

İSO–da bir sıra standartlar mövcuddur, ISO 27000 informasiya təhlükəsizliyi məsələləri üçündür [9].

ISO 27001, oktyabr 2005-ci ildə nəşr olunmuşdur, yaradılma məqsədi "İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin yaradılması və həyata keçirilməsi, əməliyyatı, monitorinqi, saxlanması və yaxşılaşdırılması üçün bir model təmin etməkdir".

ISO 27002, İSO 17799 standartının yenidən adlandırılmasıdır, "Yaradılmış təlimatlar və təşkilat daxilində informasiya təhlükəsizliyinin idarə edilməsi, həyata keçirilməsi, saxlanması və inkişaf etdirilməsi üçün ümumi prinsiplərdir."

ISO 27003 hələ təklif mərhələsindədir, məqsədi İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin həyata keçirilməsində rəhbərlik və köməklik etməkdən ibarətdir.

ISO 27005 informasiya təhlükəsizliyi risklərinin idarə edilməsi standartıdır.

ISO 27006 rəsmi adı ilə "İnformasiya texnologiyaları - Təhlükəsizlik metodları. Informasiya təhlükəsizliyinin idarə edilməsi sistemlərinin auditi və sertifikatlaşdırılmasını təmin edən təşkilatlar üçün tələblər"

Yuxarıda göstərilmiş standartlar arasında ən çox tanınan iki standartdır: İSO 27001 və İSO 27002. Digər ISO 17021, BS7799-3, ISO 24760, ISO 13335 və BS25999 kimi standartlarda bu standartlarla yaxından əlaqəlidir.

İSO 27003 standartında on bir nəzarət bəndləri mövcuddur. 1) təhlükəsizlik siyasəti; 2) informasiya təhlükəsizliyinin təşkili; 3) aktivlərin idarə edilməsi; 4) insan resurslarının təhlükəsizliyi; 5) fiziki təhlükəsizlik; 6) kommunikasiyanın idarə olunması; 7) daxil olmalara nəzarət; 8) informasiya sistemlərinin əldə edilməsi, təkmilləşdirilməsi, saxlanılması; 9) informasiya təhlükəsizliyi hadisələrinin idarə olunması; 10) biznes davamlılığını 11) uyğunluq.

IV. AUDİTİN PLANLAŞDIRILMASI

Təhlükəsizlik auditinin əsas istiqaməti aşağıdakılardır.

- Mövcud təhlükəsizlik siyasətinin, standartların, qaydalar və proseduraların yoxlanılması;
- Effektivliyin müəyyən edilməsi və mövcud siyasətin, standartların, qaydalar və proseduraların səmərəliliyinin yoxlanılması;
- Mövcud təhlükəsizlik boşluqlarının, risklərin aşkarlanması və dərk edilməsi.
- Əməliyyatlar, inzibati və idarəetmə məsələləri üzrə mövcud təhlükəsizliyə nəzarət etmək və minimum təhlükəsizlik standartlarına uyğunluğunu təmin etmək;
- Təkmilləşdirilmə üçün düzəliş və məsləhətlərin verilməsi.

Təhlükəsizlik siyasətinin uyğunluğunu təmin etmək və məqbul səviyyəyə qədər risklərin azaldılması üçün təhlükəsizlik auditi vaxtaşırı aparılmalıdır. [10] Audit özü genişləndirilmiş audit, müntəzəm audit, təsadüfi audit və ya qeyri-ofis saatlarında aparılmış audit ola bilər. Audit prosesi vaxtı avtomatik audit alətlərindən istifadə olunur (hazır təhlükəsizlik audit sistemi və ya təhlükəsizlik auditorların öz alətləri) və ya bu prosesi əl ilə etmək (sosial mühəndislik hücumları və audit yoxlama listi).

Audit prosesi bir neçə addımda yerinə yetirilə bilər. "3D Networks" yeddi addımda audit prosesi təklif edir (Şəkil 2) [11]. (1) zəifliyin aşkarlanması – strukturun yoxlanılması, (2) hesabat auditi – loqlara baxılması, (3) təhlükəsizlik arxitekturası auditi - mövcud təhlükəsizlik arxitekturanın auditi, (4) ilkin vəziyyətin auditi, (5) daxili idarəetmə və iş davamlılığı auditi – mövcud işin davamlılığının auditi, (6) siyasət auditi – iş hədəfi əsasında təhlükəsizlik siyasətinin auditi, (7) riskin auditi - müxtəlif risklərin və şirkətin kompüter sistemlərinin üzləşdiyi təhdidlərin qiymətləndirilməsi.

Audit prosesi ərzində və sonunda bir sıra hesabatlar hazırlana bilər: təşkilatın kompüter sistemində zəifliklərin aşkarlanması hesabatı, təşkilatın üzləşdiyi təhdidlər və risklərin

hesabatı. Audit hesabatı bütün audit nəticələrinin təhlükəsizlik icmalını verir.

Başqa üsulda təhlükəsizlik auditi altı audit addımlarına bölünür [15]: 1) planlaşdırma – effektiv audit metodunun müəyyənləşdirilməsi və seçilməsi üçün bütün zəruri məlumatların əldə olunması; 2) audit məlumatların toplanması – nə qədər və hansı növ informasiyanın yığılır, audit məlumatları və loqları necə süzülür və saxlanılır; 3) audit testlərinin aparılması – mövcud təhlükəsizlil siyasətinə və ya standart konfiqurasiyalara ümümi baxış; 4) audit nəticələrindən hesabat hazırlanması – cari təhlükəsizlik vəziyyətinin təqdim olunması; 5) audit məlumatlarının və alətlərinin qorunması – gələcəkdə istifadə üçün audit məlumatlarının və alətlərinin qorunması; 6) təkminləşdirmə etmək və prosesi izləmək – lazım gəldikdə düzəlişlərin aparılması. Böyüyən və mürəkkəbləşən kompüter sistemlərində audit proseslərinin yerinə yetirilməsi dahada çətinləşir. Avtomatlaşdırılmış audit alətləri əhəmiyyətli dərəcədə bu prosesi asanlaşdırır.

Şəkil 2: Audit prosesi ardıcıllığı

NƏTİCƏ

Tətbiq oluna biləcək çoxlu sayda təhlükəsizlik üsulları vardır. Təhlükəsizlik üsulu potensial riskə görə seçilməlidir. Ancaq təşkilat üçün düzgün və effektiv müdafiə qurmaq üçün kompüter sistemlərinin təhlükəsizliyi qiymətləndirilməlidir. Daxili və ya xarici təhlükəsizlik auditi təhlükəsizlik səmərəliliyini müəyyənləşdirmək üçün ən yaxşı yoldur.

Bir sıra təhlükəsizlik audit standartları vardır hansı ki, İT resurslarının adekvat qorunmasını təmin etmək üçün xüsusi proseduralar təqdim edir.

Təhlükəsizliyi qeyri-qənaətbəxş olan kompüter sistemləri böyük itkilərə gətirib çıxarda bilər, bu səbədən təhlükəsizlik auditi bütün təşkilatlarda nəzərə alınmalıdır.

ƏDƏBİYYAT

[1] Champlain .S , Auditing information systems, second ed., Hoboken, New Jersey July 2008, pp. 3 - 13

[2] Suduc .A and Filip .G, Riscuri ale utilizarii inadecvate a sistemelor informatice (Risks of Information Systems Misuse), Studii si cercetari economice, No. 72, 2008.

[3] Garg .N, Curtis .F Quantifying the Financial Impact of IT Security Breaches, Information Management & Computer Security, Vol. 11, No. 2, 2004, pp. 74-83.

[4] Manrique .L and Tacoronte .T, Supervising Employee Misuse of Information Systems in the Workplace: An Organizational Behavior Study, Empresa global y mercados locales: XXI Congreso Anual AEDEM. 1, Madrid: Universidad Rey Juan Carlos, 2007, pp. 31-43.

[5] Richardson .K, CSI Computer Crime & Security Survey, 2008, Retrieved January 2010. pp. 80-99.

[6] Lampson .P, Computer Security in the Real World, Proceedings of the Annual Computer Security Applications Conference, May 2000.

[7] Apata .J, The Essence of Information System Security and Audit. Retrieved January 2013.

[8] ITIL V3. Service Design, Office of Government Commerce (OGC), 2007

[9] ISO, The ISO 27000 Directory, 2010, Retrieved 2011

[10] OGCIO, Security Risk Assessment and Audit Guidelines, 2007, Retrieved January 2012

[11] Networks, v3, Security Audit. Retrieved 2012 February, from Scribd, Available at: http://www.scribd.com/ doc/12734608/Security-Network-Audit-Steps