İnformasiya təhlükəsizliyi baxımından kritik vəzifələr üçün tələblər sisteminin formalaşdırılması

Babək Nəbiyev

AMEA İnformasiya Texnologiyaları İnstitutu

babek@iit.ab.az

***Xülasə*— Kompüter şəbəkələrində və sistemlərində baş verən proseslərə təsir göstərən sistem administratorlarının fəaliyyətinin məqsədəuyğun aparılması üçün onların qarşısında tələblər qoyulmalıdır. Bu tələblərin yerinə yetirilməsinə nəzarət edilməsi üçün informasiya təhlükəsizliyi xidmətinin yaradılması mühüm əhəmiyyət daşıyır. Bu prosesin şəffaf olması və kompüter şəbəkələrinin və sistemlərinin iş prosesinə təsir göstərməsi üçün hər iki xidmətə xüsusi tələblər müəyyən olunmalıdır.**

Açar sözlər— sistem administratoru; informasiya təhlükəsizliyi; kompüter şəbəkəsi

I. GİRİŞ

İnternet şəbəkəsinin yayılması və sürətli inkişafı işçi yerlərin qlobal kompüterləşməsinə gətirib çıxardı. Müasir dövrdə hətta kiçik təşkilatlarda da İnternətə qoşulmuş kompüterlər var, amma bu dövrdə də kompüterlər bəziləri üçün başa düşülməyən, sadə istifadəçilər üçün isə gündəlik işlərin görülməsi üçün istifadə olunur. Bu səbəbdən kompüterlərin, kompüter şəbəkələrinin (KŞ) aparat və proqram təminatlarının təmiri və sazlanması prosesinə nəzarət olunması üçün mütəxəsislərə həmişə, hər yerdə ehtiyac duyulacaq.

Bu vəzifəni yerinə yetirən mütəxəssislər, yəni sistem administratorları (SA) kompüterlər, kompüter şəbəkələri, aparat və proqram təminatları üzrə mütəxəssislərdir. Bu mütəxəssislərin əsas vəzifələrindən biri informasiya təhlükəsizliyinin təmin olunması və təhlükəsizlik proseslərinə nəzarətdir. Bunu nəzərə alaraq, bir çox təşkilatda informasiya təhlükəsizliyi prosesinin təmin olunması, yəni təhdidlərlə mübarizə zamanı SA şəbəkə ekranlarından, müdaxilələrin aşkarlanması sistemindən və müdaxilələrin qarşısının alınması sistemindən və s. istifadə edirlər. Buna baxmayaraq, təmir, sazlanma və nəzarət funksiyalarını yerinə yetirənlər insanlardır və informasiya təhlükəsizliyinin əsas təminat xətti onlar sayılırlar [1].

Tətqiqatlarla xaker hücumları və təhdidlərin analizi zamanı müəyyən olunmuşdur ki, informasiya təhlükəsizliyinə təsir göstərən təhdidlərin çox hissəsi insan tərəfindən edilən səhvlərin nəticəsidir. Bunlara misal olaraq, müəyyən portların açıq qalmasını, şəbəkələrarası ekranda qeyri düzgün sazlanmanın aparılmasını və s. göstərmək olar. Yəni, əslində insan resurslarının edə biləcəyi səhvlərin ehtimalı avadanlıq və ya proqram təminatının boşluqlarından daha çoxdur [2]. Ona görə də baş verəcək təhdidlər kommersiya sirri, intellektual mülkiyyət, fərdi məlumatlar və s. kimi konfidensial məlumatların ələ keçirilməsinə zəmin yarada bilər. Təşkilatın profilinə uyğun olaraq SA-ya olan tələblər fərqli olmalıdır. Bu tələbləri rəhbər götürərək SA-ların iş prosesinə nəzarət və periodik audit aparılması məqsədəuyğun olardı.

SA şəbəkəni təhdid edən müxtəlif müdaxilələri aşkar etmək və onlara reaksiya vermək üçün əlamətlərə və xəbərdarlıqlara periodik nəzərət ilə yanaşı, aşkarlanmiş məlumatları əsas tutaraq düzgün və razılaşdırılmış qərar verə bilər. Bütün bu prosesin uğurlu olması SA-nın bilik səviyyəsindən asılıdır. Məsələn, tələb olunur ki, SA müdaxilələri aşkarlayan proqram təminatının təhlükələri nəyə əsasən təyin etdiyini düzgün analiz etmək qabiliyyətinə malik olsun.

II. SİSTEM ADMİNİSTRATORLARININ VƏZİFƏLƏRİ VƏ FUNKSİYALARI

SA-nın vəzifə və funksiyalarının müəyyən olunması nəticəsində praktiki fəaliyyəyin necə inkişaf edəcəyi müəyyən olunur [4]. SA İnternet-trafikin fasiləsizliyini, təşkilatın bütün informasiya aktivlərinin təhlükəsizliyini, istifadəçilərin İnternetə etibarlı və təhlükəsiz qoşulmasını, təşkilatın İnternet-trafikinə istifadə etdiyi zaman baş verən proseslərə nəzarəti təmin etməlidir. Bu baş verə biləcək təhdidlərin qarşısını almaq və şəbəkənin informasiya təhlükəsizliyi meyarlarını təmin etmək üçün olduqca əhəmiyyətlidir. Şəbəkə təhlükəsizlinin monitorinqinin (ŞTM) vəzifələrini aşağıdakı kimi izah etmək olar [3]:

a) Avadanlıq və proqram təminatı problemlərini müəyyən edərək qüsurlu komponentləri dəyişmək;
b) Məlumatların ehtiyat nüsxələrinin çıxarılması və ehtiyac olduqda bərpa edilməsi prosesini reallaşdırmaq;
c) KŞ və onunla bağlı mühitin, istifadə olunan aparat və proqram təminatının, ümumiyyətlə, sazlama prosesinin reallaşdırılması və idarə olunması;
d) Məlumatları, proqram təminatlarını və avadanlıqları qorumaq üçün şəbəkə təhlükəsizliyi tədbirlərinin reallaşdırılması və koordinasiya edilməsi;
e) Şəbəkənin qoşulması və sistemin işinin dayandırılması prosesini reallaşdıran zaman nəzarət uçotunun aparılması;
f) KŞ və sistemlərinin, əməliyyat sistemlərinin, proqram təminatlarının sazlanması və yoxlanılması;
g) KŞ və sistemlərinin inkişaf etdirilməsi və yenilənməsi prosesini aparmaq və bu barədə təkliflər və tələblər işləyib hazırlamaq;
h) KŞ-ların istifadəçiləri ilə təlim proseslərinin aparılması;

i) KŞ-ların trafikinin təşkilatın siyasətinə və tələblərinə uyğun olaraq istifadə edilməsini yoxlamaq;

j) Təmirə və ya dəyişməyə ehtiyacı müəyyən etmək üçün avadanlıq haqqında qeydlərin təhlili;

k) Şəbəkə funksiyalarına, habelə texniki xidmət və təmir qeydlərinə aid loq-faylların təhlükəsizliyinin təmin olunması;

l) Yeni texnologiyaların araşdırılması, tövsiyə edilməsi və realizəsi prosesini həyata keçirmək;

m) Sıradan çıxmış avadanlığın əvəz olunması prosesini maksimal dərəcədə az zərərli etmək.

Şübhəsiz ki, informasiya təhlükəsizliyi yüxarıda göstərilən bütün bəndlərdə nəzərə alınmalıdır, amma bu məsələlərin tətbiqi zamanı əvvəlcədən nəzərə alınması mümkün olmayan müəyyən problemlər yarana bilər. Bunlara misal olaraq lazımi kvalifikasiyalı mütəxəssislərin olmamasını, administratorun vəzifələrindən sui-istifadə etməsini və ya etməməsini göstərmək olar. Bu da nəticədə təşkilatın informasiya təhlükəsizliyinə təhdid yarada bilər.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİ XİDMƏTİ

İnformasiya təhlükəsizliyi risklərinin qəbul edilmiş səviyyədə idarə edilməsini, KŞ-in iş prinsipinin pozulmasına yönəlmiş hərəkətlərin aşkarlanmasını və qarşısının alınmasını, istifadəçilərin məlumatlandırılmasını, ziyankar proqramların yayılması və şəbəkə hücumları ilə əlaqədar statistik verilənlərin toplanmasını, saxlanılmasını və analizini təmin etmək üçün informasiya təhlükəsizliyi xidmətinin (İTX) yaradılması məqsədəuyğundur. İnformasiya təhlükəsizliyi xidməti situasiyanın analizini aparır, informasiya təhlükəsizliyinin təmin olunması üçün model hazırlayır və bu prosesin aparılması üçün tədbirlər görür. SA isə bu prosesi praktiki olaraq realizə edir. Hər bir halda iş prosesinin şəffaf və düzgün aparılması üçün İTX əməkdaşlarının bilikləri və kvalifikasiya səviyyəsi SA-dan aşağı olmamalıdır.

İTX və SA-nın arasında qarşılıqlı əlaqə aşağıda göstərilmiş dörd variant üzrə baş verə bilər:

a) İTX əməkdaşının SA kimi bütün girişlərin idarə olunması hüququ olmalıdır.

b) İTX əməkdaşı sistem inzibatçılığında, məsələn, girişlərin idarə olunması prosesində, qismən iştirak edir.

c) İTX əməkdaşının sistemin bütün konfiqurasiya-larının oxunmasına icazəsi var.

d) İTX əməkdaşının sistemə girişi yoxdur, amma sistemin loq-fayllarını, qeydiyyat jurnalını və konfiqurasiya dəyişıklıkləri haqqında məlumatları analiz edərək nəzarət funksiyasını yerinə yetirə bilər.

Bu variantlar ona görə göstərilib ki, təşkilatın profilinə görə hər iki xidmətin arasındakı münasibətlər fərqli ola bilər.

İTX təhlükəsizliyi müəyyən olunmuş qaydada təmin etmək üçün onu sistemin işləmə dövrünə inteqrasiya etməli, sistemə olan tələblərin analizi prosesinə nəzarət etməli və bütün proses periodunda təhükəsizlik qaydalarına riayət edilməsinə nəzarət etməlidir. İTX təhlükəsizliyin məqsədini (konfidensiallıq, tamlıq və əlyetənlik) müəyyən etməli və aşağıda göstərilən məsələləri həll etmək üçün qərarlar qəbul etməlidir [5]:

a) Sistemin analizinə və istifadə haqqında təlimatlara təhlükəsizlik tələbləri müyyən etməlidir.

b) Proqram təminatlarının düzgün istifadə prosesini təmin etmək üçün qaydalar müəyyən etməlidir.

c) İdentifikasiya və autentifikasiya sisteminə nəzarət etməlidir.

d) Sistem fayllarının təhlükəsizliyini təmin etməlidir.

e) İnformasiyanın ələ keçirilməməsi və ötürülməməsi üçün KŞ və kompüter sistemlərinə (KS) nəzarət etməlidir.

f) KŞ və KS-də olan boşluqların idarə olunması funksiyasını yerinə yetirməlidir.

Qəbul olunmuş qərarlar isə təşkilatın normativ sənədlərinə uyğun olaraq SA ilə icra olunmamışdan əvvəl razılaşdırılmalı, yaxud icra üçün SA-ya təqdim olunmalıdır. Amma praktikada bu elə də asan proses deyildir. Bəzi hallarda informasiya təhlükəsizliyinin təmin olunması üçün konfidensiallıq, əlyetənlilik və tamlıq funksiyalarını iki xidmət arasında bölürlər. Amma bu yalnış yanaşmadır, çünki informasiya təhlükəsizliyinin təmin olunması üçün yuxarıda göstərilən üç funksiyanı deyil, bu funksiyaların yerinə yetirilməsi üçün müəyyən mühiti və məsələləri bölüşdürmək lazımdır. Ona görə də, təşkilatda KŞ və KS-nın informasiya təhlükəsizliyi üzrə tələbləri İTX yaratmalıdır, SA isə bu tələblərə uyğun olaraq məsələləri yerinə yetirməlidir.

NƏTİCƏ

KŞ və KS-nın idarə edilməsinin və təhlükəsizliyinin təmin olunmsı prosesinə nəzarət funksiyasının yerinə yetirilməsi üçün SA-nın iş fəaliyyətinə və proseslərinə İTX əməkdaşları və ya sistemləri tərəfindən nəzarət olunmalıdır. Amma bu prosesin şəffaf və düzgün aparılması üçün hər iki xidmət üçün normativ sənədlər və tələblər müəyyən olunmalıdır. Bu proses düzgün aparıldıqda informasiya təhlükəsizliyinin təmin olunması daha effektiv həyata keçirilə bilər.

ƏDƏBİYYAT

[1] Zhen Wang, Zhijie Liu, Xiaoyao Xie, "The research of network security technologies," Anti-counterfeiting, Security and Identification in Communication, 2009, p. 585 – 587.

[2] Munir Ahmed, Lukman Sharif, Muhammad Kabir, Maha Al-Maiman, "Human Errors in Information Security," International Journal of Advanced Trends in Computer Science and Engineering v.1, no.3, p. 82-87.

[3] J. Thomas Watson, "Simplifying network administration using policy-based management ," Network IEEE, 2002, v.16, no.2, p. 20 – 26.

[4] Tang Chenghua, "Assessment of network security policy based on security capability," Communication Systems, 2008, p. 1204 – 1208.

[5] http://www.cio.ca.gov/ois/government/documents/pdf/iso_roles_respon_guide.pdf.