Azsciencenet şəbəkəsində informasiya təhlükəsizliyinin monitorinqi sistemi

Babək Nəbiyev

AMEA İnformasiya Texnologiyaları İnstitutu

babek@iit.ab.az

Xülasə— AzScienceNet elm kompüter şəbəkəsində monitorinq və təhlükəsizlik sistemi vasitəsilə hadisələr haqqında sensorlardan daxil olan məlumatların toplanması, analzi və təsnif edilməsi mühüm praktiki əhəmiyyət daşıyır. Məqalədə şəbəkə təhlükəsizliyinin monitorinqi sahəsində aparat və proqram təminatıları araşdırılmışdır. Təklif edilmiş yanaşmada AzScienceNet şəbəkəsinə uyğunlaşdırılmış informasiya təhlükəsizliyinin monitorinqi sistemi işlənib hazırlanmışdır.

Açar sözləri— informasiya təhlükəsizliyinin monitorinqi; informasiya təhlükəsizliyi; şəbəkə trafikinin analizi.

I. GİRİŞ

AzScienceNet elm kompüter şəbəkəsi (EKŞ) Azərbaycan Milli Elmlər Akademiyasının institut və təşkilatlarını elmi-tədqiqat, elmi-praktiki və tədris məsələlərinin həyata keçirilməsi üçün zəruri olan müasir şəbəkə xidmətləri ilə təmin edir.

AzScienceNet EKŞ-nın yaradılması Azərbaycan elmi-tədqiqat və təhsil mühitini Avropa elmi-tədqiqat və təhsil fəzasına inteqrasiya edərək ölkəmizdə dünya standartlarına uyğun texnologiya və xidmətlərin istifadə edilməsinə, tədqiqatçıların bu mühitdə daha səmərəli fəaliyyət göstərməsinə imkan verir.

AzScienceNet-in əsas vəzifəsi istifadəçilərinə günün 24 saatı ərzində qlobal İnternet şəbəkəsinə yüksək sürətli, təhlükəsiz çıxışı təmin etməklə yanaşı çoxsaylı xidmətlər, məsələn: AZ-CERT, hosting, AzVirtual, AzCloud, elektron poçt, elektron kitabxana, distant təhsil, eduroam və s. göstərməkdir. AzScienceNet infrastrukturunun yeni telekommunikasiya və server avadanlıqları ilə təmin edilməsi və onlar üzərindən müxtəlif İnternet xidmətlərinin göstərilməsi AzScienceNet-in dünyanın, o cümlədən Avropanın müxtəlif şəbəkə infrastrukturlarına inteqrasiyasını daha da sürətləndirmişdir.

Göstərilən xidmətlərdən göründüyü kimi, AzScienceNet heterogen infrastruktura malikdir. Bunu nəzərə alaraq, AzScienceNet-in sürətli inkişaf tempinin müxtəlif təhdidlər və nasazlıqlar nəzticəsində zəifləməməsi üçün qabaqlayıcı tədbirlər görülməlidir. Bu tədbirlər AzScienceNet-in iş prosesinin sürətinə təsir göstərmədən şəbəkədə baş verəcək təhdidlərin və nasazlıqların qaşısını almalı və operativ həll etməlidir. Bu səbəbdən şəbəkə təhlükəsizliyinin monitorinqi (ŞTM) sistemi AzScienceNet-in informasiya təhlükəsiliyi infrastrukturunda əvəzolunmaz komponentə çevrilir.

ŞTM kompüter şəbəkəsini təhdid edən müxtəlif müdaxilələri aşkarlamaq və reaksiya vermək üçün əlamətlərin və xəbərdarlıqların analizidir. Sensorların köməyi ilə kompüter şəbəkəsindən alınan məlumatlar dörd növə bölünür: təhlükəli məlumatlar, statistik məlumatlar, sessiya məlumatları və tam kontent məlumatları. Məlumatlar aşkarlandıqdan sonra ən vacib məsələ onların düzgün interpretasiyasıdır. Burada ekspertlərin hazırlıq səviyyəsi, şübhəsiz, müstəsna əhəmiyyətə malikdir. Belə olduğu halda, tələb olunur ki, təhlükəsizlik ekspertləri müdaxilələri aşkarlayan proqram təminatının təhlükələri nəyə əsasən təyin etdiyini düzgün interpretasiya etsinlər. Bu mərhələdə səhv şəbəkənin təhlükəsizliyinə nəzarətin itirilməsinə gətirib çıxara bilər [1-5].

II. AZSCIENCENET-İN ŞTM-Ə TƏLƏBLƏRİ

ŞTM-in vəzifə və funksiyalarının müəyyən olunması nəticəsində praktiki fəaliyyətin necə inkişaf edəcəyi müəyyən olunur. Bu tələblər istifadəçilərin qlobal və lokal şəbəkədən istifadəsini etibarlı və təhlükəsiz etməklə yanaşı, informasiyanın toplanaraq analiz edilməsi üçün də vacibdir [6]. Bu baş verə biləcək hadisənin qarşısını almaq və ya baş vermiş hadisəni tədqiq etmək üçün olduqca əhəmiyyətlidir. ŞTM-in vəzifələrini aşağıdakı kimidir:

a) İnternet-trafikin müşahidəsi və toplanması.

Cari seansların qeydiyyatı, istifadə olunan trafikin həcminin ölçülməsi, internet- trafikin istifadəsinə nəzarət, paketlərin tarixlə detallı qeydə alınması nəzərdə tutulur.

b) İnternet-trafikin şəbəkənin profilinə uyğunluq səviyyəsinin qiymətləndirilməsi.

İstifadə olunan Internet-trafikin istifadəçilərinin müraciətlərinin təşkilatın siyasətinə və tələblərinə uyğunluğunun yoxlanaraq konkret təsvir edilməsi nəzərdə tutulur.

c) İnternetə qoşulmuş real vaxt rejimində işləyən sistemlərin təhlükəsizliynə nəzarət.

İnternetlə bağlı real vaxt rejimində işləyən sistemlər server və kliyent tipli ola bilər. Sistemlərin təyinatına uyğun olaraq törədə biləcəyi təhlükələrin miqyası dəyişir və bu sistemləri təhlükə miqyasına görə siniflərə bölüb nəzarət səviyyəsinin xarakteristikalarını da uyğun formada nizamlamaq lazımdır.

d) İnternet istifadəçilərinin təhlükəsizliyi, konfidensiallığı və mühafizəsi.

İnformasiya təhlükəsizliyini poza bilən zərərli fəaliyyətlərin bəzi tipləri, məsələn: boşluqları olan xidmətlərə qarşı səbəkə hücumları, yüksək səlahiyyət əldə etmək üçün hücumlar, gizli məlumatların ələ keçirilməsi və ziyankar proqramların yüklənməsi həm şəbəkənin təhlükəsizliyi, həm də onun istifadəçilərinin təhlükəsizliyi və konfidensiallığı baxımından çox təhlükəlidir.

e) Sistemlərin boşluqların aşkarlanması.

Sistemlərin boşluqları onun ilkin kodunda, verilənlər bazasında, konfiqurasiyasında, idarə edilməsində ola bilər. Bu da ümumi olaraq şəbəkənin vəziyyətinə təsir göstərir.

f) Şəbəkə avadanlıqlarının diaqnostikası.

Şəbəkə avadanlıqları dedikdə, şəbəkənin işlək vəziyyətdə saxlanması üçün lazım olan qurğular (serverlər, marşutizatorlar, komutatorlar və s.) başa düşülür. Diaqnostika qurğuların yüklənmə həddi, temperaturu, informasiyanı ötürmə qabiliyyəti və s. nəzərə alınmaqla aparılır. Bu da avadanlıqlarda olan problemlər haqqında vaxtında xəbər tutaraq onların aradan qaldırılmasına imkan verir.

g) Fəaliyyətin fasiləsizliyi.

İnternet-trafikin keyfiyyətini pisləşdirəcək amillərin aradan qaldırılması və yalnız lazımi məqsədlər üçün istifadəsinə nail olmaq nəzərdə tutulur.

Beləliklə, göstərilən vəzifələrin yerinə yetirilməsi üçün sensorlardan məlumatlar toplandıqdan sonra analiz edilir və aşkarlanmış hadisələr klassifikasiya edilərək, şəbəkə təhlükəsizliyinə zərərli təsir edə biləcək hadisələr seçilir və onların təhlükə mənbəyi identifikasiya edilir. Beləliklə, istifadəçilərdən başlayaraq şəbəkənin idarəetmə mərkəzi də daxil olmaqla, monitorinq olunmalı, təhlükəsizliyə təsir edə biləcək təhdidləri izləmək lazımdır. Bu funksiyanın yerinə yetirilməsi üçün aşağıdakı məsələlərə baxılır:

a) Müəyyən olunmuş sensorlar vasitəsi ilə (SNMP, SPAN Port, NetFlow və s.) şəbəkənin vəziyyəti haqqında detallı məlumat toplanmalıdır.

b) Təhlükəsizlik sahəsində insidentlərin tapılması üçün, toplanmış informasiya analiz və korrelasiya olunmalıdır.

c) Yaranan təhlükələrə ümumi təhlükəsizlik siyasəti tətbiq olunmalıdır. Əsas monitorinqdən əlavə, müəyyən istifadəçilər üçün fərdi siyasətlər də tətbiq olunmalıdır.

d) Təhlükəsizlik sahəsində pozuntuların və zəifliklərin fasiləsiz monitorinqi aparılmalıdır. Bu tədbirlər əvvəlcədən aparılmalıdır ki, təhlükəsizlik sahəsində yarana biləcək insidentlər real təhlükə törətmədən aradan qaldırıla bilsin.

e) Təhlükə siqnallarının izlənməsi, nəzarət və ayrı-ayrı şəbəkə elementlərinin test olunması.

ŞTM-in verilənlər bazasına toplanan məlumatlardan hesabatların hazırlanması.

III. AZSCIENCENET-DƏ ŞTM-İN QURULMASI

ŞTM-in AzScienceNet-də reallaşdırılması üçün bu sahədə monitorinq sistemlərinin və vasitələrinin xüsusiyyətləri analiz edilmişdir. Monitorinq sistemlərinin və vasitələrinin əsas funksiyaları aşağıdakılardan ibarətdir: 24x7x365 rejimində şəbəkə trafikinin toplanması, toplanmış trafikin analizi və problemlərin aşkarlanması, insidentlər haqqında xəbərdarlıqların generasiyası, hesabatların yaradılması və s. ŞTM-in vastəsilə toplanmış məlumatların analizi üçün müxtəlif proqram və aparat vasitələri mövcuddur. AzScienceNet şəbəkəsi üçün aparat və proqram təminatı kompleksindən aşağıdakı optimal variant seçilmişdir.

a) Squid proxy server [7] - şəbəkə trafikinin loq-fayllarının toplanması və idarə olunması prosesini reallaşdırmaq üçün Squid proksi-serverindən istifadə edilir. Squid proksi-server açıq kodlu proqram təminatıdır və bir gün ərzində İnternetlə işləyən istifadəçilərin sayı 2000-dən çox olan böyük şəbəkələrdə istifadə olunması əlverişlidir. Squid proksi-serverin əsas üstünlüyü keşlənən proksi-server olmasıdır, bu halda müraciət olunan resurslar keşdə toplanır və onlara yenidən müraciət olunduğu halda emal prosesi operativ yaddaşda, daimi yaddaş qurğularına nisbətən daha sürətlə sona çatır. Bu da öz növbəsində şəbəkənin əlyetənliyinə müsbət təsir göstərir. Squid proksi-server vasitəsilə toplanan loq-fayllar xüsusi verilənlər bazasında toplanaraq analiz prosesində istifadə olunur.

b) WebSpy Vantage [8] - bu proqram vasitəsi ilə proksi-serverdə toplanan loq-faylları oflayn analiz etmək mümkündür. Bu proqram 200-dən çox loq-fayl və hadisə jurnalı tipini dəstəkləyir, beləliklə, zəruri olduqda digər tip loq-fayl və hadisə jurnalı tiplərini də analiz etmək imkanı yaradır. Ümumi şəbəkənin və istifadəçilərin tək və ya qrup halında monitorinqini həyata keçirir. Bu zaman şəbəkə seqmentləri (VLAN) üzrə hesabat, veb-saytlar üzrə hesabat, IP-ünvanlar üzrə hesabat, verilənlərin tipi üzrə hesabat, veb-saytların profilinə görə trafikin paylanması, ölkələr üzrə hesabat, həftənin günləri üzrə hesabat, günün saatları üzrə hesabat və s. əldə etmək mümkündür.

c) SpamTitan [9] – e-poçt xidmətinin anti spam və monitorinq sistemidir. Monitorinq xidməti üçün gündəlik, həftəlik, aylıq və illik avtomatik hesabarlar (e-poçt və ya PDF formatında) yarada bilir. Elektron məktublar iki antivirus sistemi (ClamAV və Kaspersky) tərəfindən yoxlanır və antivirus bazası periodik yenilənir.

d) CACTİ [10] – açıq kodlu proqram təminatı olub, kompüter şəbəkəsi trafikinin, qovşaqların vəziyyətinin və avadanlıqlar haqqında statistik informasiyanı müəyyən vaxt intervalında SNMP vasitəsilə toplayaraq qrafiklər yaradır.

e) Cisco ASA və onun CSC-SSM modulu [11] – yüksək hesablama gücünə malik avadanlıqdır, trafikin süzülməsi, viruslardan, soxulcan və müxtəlif tipli İnternet hücumlarından müdafiəni, korparativ şəbəkənin perimetrinin təhlükəsizliyini, VPN-lə qoşulma zamanı IPSec şifrləmə protokolunu dəstəkləyir. Təhdidlərin aşkarlanması bazasında 25000-dən çox siqnatur var bu baza vaxtaşırı yenilənir.

NƏTİCƏ

AzScienceNet-də informasiya təhlükəsizliyinin təmin edilməsi və monitorinq aparılması üçün ŞTM şəbəkə infrastrukturu və onun bütün elementləri ilə inteqrasiya olunmalıdır. Quraşdırılmış aparat və proqram təminatı sistemlərinin yenilənən bazaları olduğu üçün təhlükələri aşkarlamaq imkanları genişlənir və onlarla mübarizə şəbəkənin müxtəlif səviyyələrində aparıla bilir. ŞTM arxitekturu bütün elementləri ilə birlikdə yüksək nəzarətli infrastruktur formalaşdırır. Bu mexanizm daim dəyişən və inkişaf edən təhlükələrə qarşı şəbəkənin proaktiv mühafizəsinin bilavasitə güclənməsinə kömək edir və eyni zamanda şəbəkənin etibarlılığını yüksəldir.

ƏDƏBİYYAT

[1] М.И. Мельников, "Автоматизированная система мониторинга по сетям TCP/IP," *Доклад Томский государственный университет систем управления и радиоэлектороники*, № 2 (18), с.98-100, 2008.

[2] Г.А.Андрианов, К.Е.Самуйлов, Ю.В.Гайдамака, "Анализ модели трафика ОКС-7 по результатам обработки статистики измерений," *Журнал «Вестник связи»*, №11, с. 17-23, 2007.

[3] Н.Г.Булахов, "Методы обнаружения компьютерных вирусов и сетевых червей," *Научная сессия ТУСУР*. Томск : В-Спектр, 2008, с. 39-41.

[4] Brian A. LaMacchia, Sebastian L., Matthew L., Rudi M., Kevin T. Price, "*.NET framework security*," Boston: Addison-Wesley, 2002, 816 p.

[5] Артамонов В. А., Лепешкин О. М., "Подход к реализации сетевой системы обнаружения аномалий на основе реконструкции модели сетевого трафика," *Инфокоммуникационные технологии*, № 3, с. 145-147, 2007.

[6] В.А.Васенин, С.А.Афонин, А.Ф.Слепухин, "К созданию системы сетевого мониторинга," *Всероссийская научно-методическая конференция "ТЕЛЕМАТИКА'99"*, СПб.: СПбГУ ИТМО, с.54-56, 1999.

[7] http://ru.wikipedia.org/wiki/Squid

[8] http://www.softcode.com.tr/markalar/webspy/VantageUltimateDatasheet.pdf

[9] http://www.spamtitan.com/solutions/for-education

[10] http://www.cacti.net/what_is_cacti.php

[11] http://www.cisco.com/web/RU/solutions/smb/products/security/asa_5500_series_adaptive_security_appliances.html