İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərinin analizi

Rəşad Həmzəyev[1], Tural Məmmədov[2]

AR XDMX Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi

[1]rashad@dmx.gov.az, [2]mammadov.t@dmx.gov.az

***Xülasə*— Hüquqi və fiziki şəxslərin, dövlət və özəl müəssisələrin informasiya texnologiyalarından asılı olduğu bir zamanda informasiya təhlükəsizliyi insidentləri qaçılmazdır. Geniş istifadə olunan əməliyyat sistemlərində təhlükəsizlik təmin olunsa da, təhdidlərdən tam müdafiəyə zəmanət verilmir. Kompüter sistemlərinin getdikcə mürəkkəbləşməsi insidentlərlə mübarizəni daha da kəskinləşdirir. Bu məqalədə informasiya təhlükəsizliyi insidentlərinin emalı üzrə müxtəlif metodologiyalar və proseslər müqayisəli analiz edilir.**

Açar sözlər*— *informasiya təhlükəsizliyi; informasiya təhlükəsizliyi insidenti; insidentin emalı

I. GİRİŞ

İnformasiya təhlükəsizliyi insidentlərinin emalı haqqında danışmazdan öncə,insidentlərin emalı prosesi ilə məşğul olan "CSIRT" (Computer Security Insident Response Team) qurumlarına nəzər salaq. Bu qurumların xidmət aspektləri, insidentlərin təsnif edilməsi və emalı proseslərinə yanaşma tərzləri və digər parametrləri bir-birindən fərqlənir. CSIRT-lər xidmət göstərdikləri fəaliyyət sahəsinə və istifadəçilərinə görə dövlət, milli, akademik, biznes, qurumdaxili (ing. self-service) olmaqla bir neçə qrupa bölünür. CSIRT-in yaradılması və fəaliyyətə başlaması ilk öncə onun fəaliyyət və xidmət sahəsinin, o cümlədən istifadəçilərinin seçilməsi ilə başlayır ki, bu da aşağıda göstərilən parametrlərin seçilməsi ilə müəyyən edilir:

- IP (Internet Protocol) silsilələri;
- Avtonom sistem (ing. Autonomous system) nömrələri;
- Domen adları və ya zonası;
- Mətn formatlı təsvir;

Xidmət sahəsi və istifadəçilərin müəyyənləşdirilməsindən sonrakı əsas mərhələ həmin istifadəçi qruplarının kommunikasiya vasitələri ilə təmin etmək CSIRT-in müraciət etməklərini təmin edəcək kommunikasiya vasitələrinin istifadəçilərə çatdırılması və CSIRT-in istifadəçilərə tanıdılaraq onların etimadını qazanması prosesidir. Burada kommunikasiya vasitələri istifadəçilərin qarşılaşdıqları insidentləri emal etmək üçün CSIRT-ə müraciətlərini təmin edir.

CSIRT-lərin göstərdikləri xidmətləri əsasən 3 qrup altında birləşdirmək olar:

1. *Reaktiv xidmətlər* – xəbərdarlıqlar, insidentlərin analizi və emalı, boşluqların analizi və emalı, artifakt analizi və emalı;
2. *Profilaktik xidmətlər* – elanlar, texnoloji yeniliklər, təhlükəsizliyin dəyərləndirilməsi və auditi, təhlükəsizlik vasitələrinin və infrastrukturunun konfiqurasiyası və sazlanması, təhlükəsizlik alətlərinin yaradılması, müdaxilənin aşkarlanması, təhlükəsizlik ilə bağlı xəbərlərin yayılması;
3. *Təhlükəsizlik səviyyəsinin idarə edilməsi* – risk analizi, fəaliyyətin davamlılığının təmini və fövqaladə vəziyyətdə bərpa mexanizmi, təhlükəsizlik konsaltingi, maarifləndirmə tədbirləri, təhsil və təlimlər, məlumatın qiymətləndirilməsi və ya sertifikatlaşdırma.

İnsidentin emalının uğurlu nəticələnməsi üçün vacib *amillərdən* biri CSIRT-in əməkdaşlarının iş bölgüsü və rollarının düzgün müəyyənləşdirilməsidir. CSIRT virtual və ya fiziki, qurumdaxili və ya beynəlxalq, biznes xarakterli və ya akademik, dövlət və ya milli fəaliyyət növlərinin birinə uyğun xidmət göstərə bilər. Bütün bunlar nəzərə alınaraq, CSIRT-dəki işlərin və əməkdaşların işlərə uyğun olaraq düzgün bölüşdürülməsi və onların bu prosesdəki rollarının CSIRT-in missiyasına, xidmət sahəsinə və istifadəçilərinə uyğun formada müəyyənləşdirilməsi insident emalının uğurlu nəticəsindəki əsas amillərdən biridir.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİNİN EMALI PROSESLƏRİ

İnformasiya təhlükəsizliyi insidentlərinin emalı çox mərhələli bir prosesdir. Bu çox qəliz mərhələlərdən də keçə bilər sadə qısa mərhələli bir həll modeli ilə də emal oluna bilər. Dünyada bir çox İnsident emalı modelləri var. CSIRT praktikasında ən çox istifadə olunan modellərdən birini ətraflı araşdıraq. Bu model adı ilə məhşurdur və insidentlərin emalı 4 əsas mərhələdə gerçəkləşir:

1. İnsidentin aşkarlanması (və qeydiyyatı): İnsident haqqında məlumat verilir və ya insident hər hansı bir araşdırma vasitəsilə və ya alətlə aşkarlanır.
2. İnsidentin sinifləndirilməsi (ing. triage): İnsident qiymətləndirilir, sinifləndirilir, prioriteti müəyyən olunur və emal üçün bilet(ticketing) açılır.
3. İnsidentin analizi: İnsident araşdırılır, baş verənlər müəyyənləşdirilir, insidentin təsir sahəsi analiz olunur.
4. İnsidentin bağlanması (ing. insident closure): İnsident emal edilir, problem həll olunur, nəticə haqda məlumat verilir.

Bu mərhələlərin ətraflı analizi aşağıdakı kimidir.

III. İNSİDENTİN AŞKARLANMASI

İnsident haqqında məlumat iki yolla əldə edilir: Siz ya insidenti şəxs tərəfindən xüsusi araşdırma və ya alətlər vasitəsilə aşkar edirsiniz və ya insident haqqında kənardan məlumat daxil olur. Bu iki mərhələnin sxematik təsviri şəkil 1-də verilir.

Şəkil 1. İnsidentin aşkarlanması sxemi

İlk növbədə daxil olan məlumatın real olub-olmaması yoxlanılır. Daha sonra məlumat verilən insidentin CSIRT-in xidmət sahəsinə aid olub-olmadığı müəyyən edilir. Əgər insident CSIRT-in xidmət sahəsinə aid deyilsə, tanıdığı digər CSIRT-in xidmət sahəsidirsə, insident barədə onlar məlumatlandırılır. Burda ən vacib məsələlərdən biri insident barədə digər qurum və ya CSIRT-i məlumatlandırarkən konfidensiallığa riayət olunması məsələsidir. Bu mövzu növbəti mərhələlərdə ətraflı şərh olunur. Əgər insident CSIRT-in xidmət sahəsinə aiddirsə, o zaman bu insident barədə daha öncə məlumat verilib-verilmədiyi yoxlanılır. Əgər insident barədə təkrar məlumat daxil olursa, həmin insident daha öncə daxil olmuş insident ilə əlaqələndirilir. Əgər insident yenidirsə, o qeydiyyata alınır və növbəti mərhələlərə yönləndirilir. Qeydiyyat mərhələsi burada ən əsas məsələlərdən biridir. Qeydiyyat üçün xüsusi insident qeydiyyatı proqramlarından istifadə edilə bilər və ya CSIRT öz sistemini yarada bilər. Əsas məsələ sistemin asan başa düşülən olması, sistemdə bir çox seçimlərə görə süzgəcləmə imkanının olmasıdır. Süzgəcləmə insidentlərin araşdırılması, analizi, bir-biri ilə əlaqəsinin müəyyən edilməsi baxımından ən çox istifadə olunan alətlərdən biridir. İnsidentlərin qeydiyyat proqramı veb texnologiyalara əsaslanırsa, onun təhlükəsizliyi (informasiya sızması və s.), kənar müdaxilələrdən və spamlardan qorunması diqqətə alınması vacib olan əsas məsələlərdən biridir.

IV. İNSİDENTİN SİNİFLƏNDİRİLMƏSİ

"Triage" sözü fransız dilindən götürülmə bir söz olub, tibbi termindir. Mənası məhdud imkanlarla xəstələrə ilkin diaqnoz qoymaq və xəstələri xəstəliyin ağırlığına görə qruplaşdıraraq növbəyə qoymaqdır. Məhz insidentə yanaşma da bu tərzdə aparılmalıdır. Bütün bu mərhələlərə bir-bir nəzər yetirək.

– İlk öncə əldə edilmiş insidentin doğruluğu və CSIRT-in xidmət sahəsinə aid olması müəyyən edilir.
– Daha sonra insindentin növü müəyyənləşdirilir və insident sinifləndirilir. Adətən, ilkin sinifləndirmə ya insident haqqında məlumat verən tərəfindən, ya da insidenti qəbul edən tərəfindən aparılır.
– Növbəti addım qeydiyyata alınmış insidentin vaciblik dərəcəsini müəyyənləşdirməkdir. Vaciblik dərəcəsinin müəyyənləşdirilməsində bir çox vasitələrdən istifadə edilə bilər. Bunlardan biri də kart sistemidir. Kart sistemi iki formada qurula bilər. Bunlardan biri insidentin ciddiliyinə, vacibliyinə görə olan sinifləndirmədir (cədvəl 1).

CƏDVƏL 1. İNSİDENTİN VACİBLİYİNƏ GÖRƏ İNSİDENT SİNİFLƏRİ

Grup Kartı	Vaciblik Dərəcəsi	Nümunə İnsidentlər
Qırmızı Kart	Çox Yüksək	DDoS, pishing resurslar
Sarı Kart	Yüksək	Troyan yayılması, İnformasiyaya kənar müdaxilə
Narıncı Kart	Orta	Spam, müəllif hüquqları məsələləri

Digər kart sistemi isə xidmət sahəsinin və ya istifadəçilərin vaciblik dərəcəsinə görə kart sinifləndirməsi sistemidir (cədvəl 2).

CƏDVƏL 2. İSTİFADƏÇİLƏRİN VACİBLİYİNƏ GÖRƏ İNSİDENT SİNİFLƏRİ

Grup Kartı	Dövlət Qurumları	SLA müştərilər	Digər
Qırmızı Kart	1	1	2
Sarı Kart	1	2	3
Narıncı Kart	2	3	3

– Nəhayət, insidentin sinifləndirilməsi prosesində sonuncu mərhələ insident tapşırığının hazırlanmasıdır. Bunun üçün əldə edilən bütün informasiya təsnif edilərək qeydiyyata alınır və insident tapşırığı olaraq insident emalı üçün növbəti mərhələyə ötürülür.

V. İNSİDENTİN ANALİZİ

İlkin sinifləndirmədən sonra növbəti mərhələ analiz və qərar mərhələsidir.Bu mərhələ daha uzun çəkən bir araşdırma prosesindən keçir ki, bəzən nəticə əldə etmək üçün bu prosesi bir neçə dəfə təkrar keçmək lazım gəlir. Proses 5 mərhələdən ibarətdir: məlumatların təhlili, qərarın tədqiqi, müəyyən fəaliyyət planının təklifi, fəaliyyət planının həyata keçirilməsi, insidentin aradan qaldırılması və zərərin bərpası.

- ***Məlumatların təhlili:*** Məlumatın təhlili zamanı ilkin görüləcək iş, əlaqədar tərəfləri məlumatlandırmaq və onlardan lazımı məlumatları əldə etməkdir. Çünki insident haqda məlumat verənlər həmişə insidentdən zərərçəkmiş tərəflər olmur. Bir çox hallarda insidentdən zərəçəkmiş tərəfin insidentin baş verməsindən xəbəri olmur, insident haqqında məlumat 3-cü tərəf vasitəsi ilə alınır. Tərəflərin məlumatlandırılması zamanı onlara insident barədə ilkin məsləhətlər və insidentin aradan qaldırılması üçün görüləcək işlər barədə ilkin məlumat verilə bilər. İnsident təhlili üçün əsas məsələlərdən biri tərəflərdən mümkün qədər maksimum informasiya əldə etməkdir. Bu informasiya insidentin baş verməsinin detallarının açıqlanması, əlaqə vasitələri, loqlar, insidentin dəqiq başvermə zamanı,

əməliyyat sistemləri, şəbəkə sazlamaları, təhlükəsizlik vasitələrindən (məsələn, antivirus, şəbəkələrarası ekran) istifadə və s. ola bilər.

- ***Qərarın tədqiqi:*** Qərarın tədqiqi zamanı əsas faktorlardan biri bu tipli insidentlə əvvəlcə qarşılaşmaqdır. Əgər bu tipli insident daha öncə baş veribsə, bu insident haqqında qeydiyyat bazasında əldə edilmiş praktik bilgilərdən qərarın tədqiqi prosesində istifadə etmək mümkündür. Əgər bu sahədə praktik bilgilər yoxdursa, baş vermiş insidentlərin araşdırılmasına və digər CSIRT-lərin praktik bilgilərindən faydalanmağa ehtiyac yaranacaq.
- ***Müəyyən fəaliyyət planının təklifi:*** Bu mərhələdə qəbul edilmiş hər bir konkret və praktiki tapşırıq insidentdə iştirak edən bütün tərəflərə çatdırılmalıdır. Hədəf tərəf texniki əməkdaş olmaya da bilər və təqdim edilmiş təkliflərdən heç nə anlamaya bilər. Buna görə də təkliflər və atılacaq addımlar yuxarıda daha öncə göstərilən, məlumatlandırılması lazım olan tərəflərə onların anlayacağı formada və aidiyyatı məlumatlar olmaq üzrə çatdırılmalıdır.
- ***Fəaliyyət planının həyata keçirilməsi:*** CSIRT-in qərarının və təkliflərinin nə olmasından asılı olmayaraq bir məsələni bilməlidir ki, CSIRT-in başqalarının nə edəcəyinə qərar vermək üçün səlahiyyətləri məhduddur. Optimistik yanaşma odur ki, bütün tərəflər CSIRT-in təklifi ilə razılaşacaq və CSIRT-in dediklərini yerinə yetirəcək. Bütün bunlarla yanaşı bəzi ilkin yoxlama vasitələri var ki, CSIRT bu vasitələrlə fəaliyyət planının həyata keçirilməsinə nəzarət edə bilər. Fəaliyyət planının həyata keçirilməsinə nəzarət aşağıdakı sualları cavablandırmaqla müəyyən edilə bilər: Hücumun hədəfləndiyi xidmət aktiv və ya deaktivdir? Hücumun hədəfləndiyi xidmətdə mövcud boşluqlar aradan qaldırılıb ya yox? Süzgəclənməsi nəzərdə tutulan trafik hələ də şəbəkədə özünü göstərir ya yox?
- ***İnsidentin aradan qaldırılması və zərərin bərpası:*** Bütün görülən işlərin bir əsas məqsədi var: insidentin aradan qaldırılması və zərərin bərpasıdır. Yəni hər hansı bir xidmətə və ya sistemə hücüm olmuşdursa, insidentin aradan qaldırılması sistemin əvvəlki işlək vəziyyətinə qaytarılması və faəliyyətinin fasiləsizliyinin təmin edilməsidir.

VI. İNSİDENTİN BAĞLANMASI

Analiz və qərar mərhələsində uzun çəkən araşdırma prosesindən sonrakı mərhələ insidentin bağlanmasıdır. Bu mərhələ aşağıdakılardan ibarətdir:

- ***Yekun məlumatlandırma:*** İnsidentin bağlanması zamanı insident haqqında qısa məlumat, görülən tədbirlərin nəticəsi, aşkarlanan əsas boşluqlar və məsləhətlər yazılaraq tərəflərə ötürülməli və insidentin bağlanması barədə tərəflər məlumatlandırılmalıdır.
- ***Yekun siniflәndirmə:*** Burada üç bənd nəzərdə tutulur: 1) insident barədə ilkin məlumat alarkən, o ya məlumat verənin informasiyasına əsasən, ya da insidenti qəbul edənin praktik bilgilərinə əsasən sinifləndirilməlidir. 2) insidentin təhlili zamanı müəyyən olunur ki, insident əslində qeyd olunduğu kimi deyil, başqa bir qrupa, başqa sinifləndirməyə aiddir. 3) insident emal olunduqdan sonra onun gələcəkdə daha asan tapılması üçün bütün aspektləri nəzərə alınaraq sinifləndirilməsi dəyişdirilmir.
- ***Arivləşdirmə:*** İnsident bağlandıqdan sonra onu arxivləşdirmək lazım gəlir. Arxivləşdirmə əməliyyatı elə aparılmalıdır ki, gələcəkdə oxşar insidentlər baş verdikdə həmin insident numünə kimi arxivdə daha rahat axtarılan və məlumatlar daha əlçatan olsun. Bunun üçün arxivləşdirmədə insidentin klassifikasiyasına, qeydiyyat tarixinə və parametrlərə görə süzülməsini təmin etmək lazımdır. Təbii ki, arxivləşdirmə zamanı nəzərə alınacaq digər məsələ backup və şifrləmə əməliyyatıdır. Yadda saxlamaq lazımdır ki, insidentin emalı zamanı istifadə olunan məlumatlar konfidensial məlumtlardır. İnsidentin klassifikasiyaya uyğun arxivləşdirilməsi aşağıdakı CSIRT-taksonomiyaya uyğun aparıla bilər.

İnsidentin adı	İnsidentin növü	İzah / Nümunə
Narahatedici kontent	Spam	Spamların göndərilməsi və ya qəbul edilməsi
	Təcavüz	Nüfuzdan salma və ya diskriminasiya
	Uşaq/porno/şiddət...	Uşaq pornosu, şiddətin yayılması
Ziyankar kodlar	Virus Worm Trojan Spyware Dialler	Sistemə bilərkən sızdırılmış zərərvericilər
İnformasiyanın toplanması	Skanlama	Sistemin xüsusi skanerlər vasitəsilə analiz edilib boşluqlarından istifadə edilməsi
	Sniffer	Şəbəkə trafikinin izlənməsi və qeydiyyatı
	Sosial Mühəndislik	İnformasiyanı texniki vasitələrdən istifadə etmədən, insan faktorundan yararlanaraq əldə etmək
Hücum cəhdləri	Məlum eksploytlar	Məlum exploitlərin köməyi ilə maneələrin keçilməsi
	Loqin cəhdləri	Parolun sındırılması, kobud qüvvələr (brute force) və bu kimi loqin cəhdləri
	Yeni hücum signaturaları	Siqnaturları naməlum exploytlarla maneələrin keçilməsi
Hücum	İstifadəçiimtiyazlarının artırılması	İcazəsiz giriş izninin əldə edilməsi
Xidmətin fasiləsizliyi	DoS DDoS	Botlardan istifadə edərək süni yüklənmənin yaradılması
	Sabotaj	Elektrikin kəsilməsi və s.
İnformasiyanın təhlükəsizliyi	İnformasiyaya icasəsiz müdaxilə İnformasiyanın icazəsiz modifikasiyası	Wiretapping, spufinq, hijacking və bu kimi vasitələrdən istifadə edərək informasiyaya icazəsiz müdaxilə
Dələduzluq	Resursdan icasəsiz istifadə	Resursdan icazəsiz istifadə və pul qazanma
	Müəllif hüquqları	Lisenziyasız vasitələrdən istifadə və müəllif hüquqlarını pozma
	Maskarad	Kiminsə adından istifadə etmək
Digər	Yuxarıdakı kateqoriyalara uyğun olmayan bütün insident tipləri	

İnsidentlərin tipləri, növləri genişləndikcə təbii ki, bu cədvəldəki taksonomiya da uyğun olaraq genişləndirilə bilər.

VII. İNSİDENTLƏRİN EMALINDA DİQQƏT EDİLMƏLİ MƏQAMLAR

Sonrakı analiz: Emal edilmiş insidentlər bağlandıqdan müəyyən müddət sonra onların yenidən analizinin aparılmasını nəzərdə tutur. Bu əməliyyatın aparılması müəyyən praktiki biliklər qazanmağa, həm də əvvəllər nəzərə çarpmayan səhvlərin müəyyənləşdirilməsini təmin etməyə imkan verir.

İnformasiyanın məxfiliyi *(ing. information disclosure):* Gündəlik fəaliyyəti zamanı qarşılaşdığımız informasiyaların hər biri nə dərəcədə fərqinə varmasanız belə, çox konfidensial məxfi informasiyalardır. Təbii ki, bu informasiyalarla işləmək onların məxfiliyini qorumaq və onlarla ehtiyatlı davranmaq CSIRT-in həm etimad göstəricisi, həm də professionallığını göstərən əsas amillərdən biridir.

İşıqfor protokolu *(Traffic Light Protocol):* Bu protokol bütün dünya CSIRT-ləri tərəfindən istifadə edilən və informasiyanın məxfilik dərəcəsini göstərən nişanlama vasitəsidir. Bu protokol aşağıda şəkildə izah edilmişdir.

CƏDVƏL 3. İŞIQFOR PROTOKOLU

RED	Paylanılması icazə verilməyən məxfi məlumat. Bu məlumat, məlumatın hazırlanması prosesində iştirak edən iştirakçılardan başqa heç bir əməkdaş və ya qurum arasında paylaşıla bilməz. Məlumatın paylana bilinməsi üçün bütün iştirakçı tərəflərin imzası tələb olunur.
AMBER	Paylanması məhdud dərəcəsə icazə verilən məxfi məlumat. Bu məlumat ancaq iştirakçıların aid olduqları qurum üzvləri arasında paylaşıla bilinər.
GREEN	Məlumat aidiyyatı qurumlara paylanıla bilər ancaq məlumatın ictimailəşdirilməsi qadağandır.
WHITE	Məlumat ictimaiətə açıq məlumatdır, istənilən şəxs və ya istənilən qurum məlumatı paylaşa bilər.

ƏDƏBİYYAT

1. XRİTDA - Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi http://cert.gov.az/
2. ENISA- European Network and Information Security Agency http://www.enisa.europa.eu/
3. TERENA – Networking of Networker http://www.terena.org/
4. European CSIRT Network http://www.ecsirt.net
5. The Trusted Introducer- European CSIRTs Community http://www.trusted-introducer.org/
6. CERT / CC –Carnegie Melon Univercity of http://www.cert.org/
7. DerbyShire Country Council http://www.derbyshire.gov.uk