İnformasiya Sistemlərində Hücum Səthinin İdarə Olunması və Müasir Kibertəhlükəsizlik Modellərinin İnteqrasiyası

Rəvan Rəsulzadə[1], Lamiyə Nəcəfova[2]
[1]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[2] Riyaziyyat İnstitutu, Bakı, Azərbaycan
[1]*ravanrasulzada@gmail.com*, [2]*najafova.lamiya@gmail.com*

Xülasə– **Məqalədə hücum səthinin idarə olunması və sıfır etibar modellərinin qarşılıqlı inteqrasiyası tədqiq edilmişdir. Tədqiqat işində aktivlərin aşkarlanması, monitorinqi və risklərin kəmiyyət göstəriciləri ilə qiymətləndirilməsi üçün CVSS 4.0, EPSS və FAIR metodologiyalarına əsaslanan proaktiv model təklif edilmişdir. Təklif edilən modeldə CVSS 4.0, EPSS və FAIR kimi müasir risk qiymətləndirmə metodologiyalarına əsaslanan yeni riyazi model və sistem arxitekturasından istifadə edilmişdir.**

Açar sözlər - hücum səthinin idarə olunması; sıfır etibar; kibertəhlükəsizlik riskləri; kölgə informasiya texnologiyası; risk qiymətləndirilməsi

I. GİRİŞ

Müasir dövrdə rəqəmsal transformasiya proseslərinin intensivləşməsi informasiya sistemlərinin arxitekturasında böyük dəyişikliklərə səbəb olmuşdur. Bulud texnologiyalarının (Cloud Computing), əşyaların internetinin (IoT) və mərkəzsizləşdirilmiş iş modellərinin kütləvi tətbiqi ənənəvi "perimetr əsaslı müdafiə" strategiyasını effektivsizləşdirərək, korporativ şəbəkələrin sərhədlərini qeyri-müəyyən etmişdir. Bu təkamül fonunda, informasiya sistemlərinin təhlükəsizlik arxitekturasında "hücum səthi" (Attack Surface) anlayışı kibertəhdidlərin analizi və idarə olunması üçün episentrə çevrilmişdir.

Hücum səthi hakerin sistemin konfidensiallığına, bütövlüyünə və ya əlçatanlığına xələl gətirmək üçün istifadə edə biləcəyi bütün ekzogen və endogen giriş nöqtələrinin, aktivlərin və zəifliklərin məcmusudur [1]. Problemin aktuallığı ondan ibarətdir ki, dinamik və hibrid infrastrukturlarda kiber-aktivlərin (IP ünvanları, API son nöqtələri, SSL sertifikatları və s.) sayı həndəsi silsilə ilə artmaqdadır. Beynəlxalq araşdırmalar göstərir ki, müəssisələrin rəqəmsal aktivlərinin təxminən 30%-i " Kölgə informasiya texnologiyaları (bundan sonra – Kölgə İT (Shadow IT)) kateqoriyasına daxil olaraq mərkəzləşdirilmiş təhlükəsizlik monitorinqindən kənarda qalır. Bu naməlum aktivlər hakerlər üçün "ən az müqavimət yolu" yaradaraq, kritik infrastrukturun iflic edilməsinə şərait yaradır.

II. KÖLGƏ İNFORMASİYA TEXNOLOGİYALARININ KİBER-MÜDAFİƏ ARXİTEKTURASINDA YARATDIĞI RİSK VEKTORLARI

Kölgə İT–müəssisənin İT şöbəsinin xəbəri, icazəsi və ya nəzarəti olmadan işçilər tərəfindən istifadə edilən hər hansı texnoloji həlldir. İT şöbəsi şirkətdəki bütün rəsmi proqramları və cihazları "işıqlandırır" (yəni monitorinq edir, yeniləyir və qoruyur). Lakin işçilər rəsmi icazə almadan kənar bir alət istifadə etdikdə, həmin aktiv İT şöbəsinin "müşahidə sahəsi" çıxır və kölgədə qalır. İnformasiya təhlükəsizliyi iyerarxiyasında Kölgə İT ekosistemi "ən zəif halqa" (*the weakest link*) paradiqmasını təmsil edərək, müəssisənin kiber-dayanıqlığı üçün aşağıdakı bir neçə fundamental risk vektorlarını formalaşdırır:

A. Verilənlərin eksfiltrasiyası və inzibati nəzarət mexanizmlərinin deqradasiyası

Korporativ məlumatların müvafiq icazə olmadan şəxsi bulud saxlanc sistemlərinə (məsələn, *Dropbox, Google Drive*) ötürülməsi, məlumatın həyat dövrü (*data lifecycle*) üzərindəki inzibati nəzarəti ləğv edir. Bu halda, işçi ilə əmək münasibətlərinə xitam verildikdə belə, kritik korporativ verilənlər müəssisənin nəzarət zonası xaricində qalır ki, bu da sızma riskini multiplikativ şəkildə artırır.

B. Yamaq idarəetməsinin qeyri-mümkünlüyü:

İT departamentinin müşahidə sahəsi xaricində olan proqram təminatları mərkəzləşdirilmiş yenilənmə və yamaqların idarəolunması (Patch Management) proseslərindən məhrum olur. Köhnəlmiş konfiqurasiyalar və kritik zəifliklər (CVE) olan tətbiqlər, hakerlər üçün şəbəkə daxilinə sızmaq üçün açıq giriş nöqtəsinə çevrilir.

C. Normativ-hüquqi çərçivələrə uyğunluq və requlyativ defisit

Kölgə İT ekosisteminin nəzarətsiz şəkildə genişlənməsi müəssisənin milli və beynəlxalq normativ-hüquqi çərçivələrə uyğunluq səviyyəsini ciddi şəkildə zəiflədir. İT departamentinin təsdiqindən keçməyən proqram və xidmətlər informasiya təhlükəsizliyi siyasətləri, məlumatların qorunması standartları və audit tələbləri ilə inteqrasiya olunmadığından, təşkilatda requlyativ boşluqlar (compliance gaps) formalaşır. Nəticə etibarilə, ISO/IEC 27001, GDPR və digər uyğunluq mexanizmlərinin tələb etdiyi məlumatların məxfiliyi, bütövlüyü və izlənəbilənliyi prinsipləri pozulur. Bu isə audit uyğunsuzluqları, hüquqi məsuliyyət, maliyyə sanksiyaları və reputasiya itkisi risklərini əhəmiyyətli dərəcədə artırır.

D. İnsidentin aşkarlanma müddəti

Ən əsası isə təhlükəsizlik əməliyyatları mərkəzi (SOC) üçün

DOI: 10.25045/forensic.gov.2026.69

görünməyən hər bir aktiv, monitorinq sistemlərində "müşahidədən kənar sahə" yaradır. Hücumçu kölgədə qalmış bir resurs vasitəsilə lateral hərəkət etdikdə, insidentin aşkarlanma müddəti kəskin şəkildə artır ki, bu da hakerə sistemi komprometasiya etmək üçün kifayət qədər vaxt qazandırır.

III. Hücum Səthinin İdarə Olunması Prosesinin Funksional Mərhələləri

Hücum səthinin idarə olunması (bundan sonra - HSİO) statik bir əməliyyat deyil, davamlı təkmilləşən dinamik bir dövrdür. Bu proses aşağıdakı dörd fundamental mərhələni əhatə edən sinergetik bir vəhdətdən ibarətdir:

- Aşkarlama (Discovery): Passiv və aktiv skanlama metodologiyalarından istifadə edərək, təşkilatın internetə çıxışı olan bütün rəqəmsal izlərinin (DNS qeydləri, IP blokları, SSL sertifikatları) tam inventarizasiyası həyata keçirilir.
- Təhlil (Analysis): Aşkarlanmış aktivlərin proqram təminatı stack-i, konfiqurasiya xətaları və istismar müddəti bitmiş (End-of-Life) komponentləri müəyyən edilərək texnoloji vəziyyəti təhlil olunur.
- Prioritetləşdirmə (Prioritization): Müəssisənin risk iştahına və aktivin biznes əhəmiyyətinə uyğun olaraq, hər bir boşluq üçün kəmiyyət risk balı hesablanır.
- Monitorinq (Monitoring): Sistem davamlı monitorinq həyata keçirilərək, hücum səthində baş verən hər bir dəyişiklik və ya yeni "Shadow IT" aktivi real-vaxt rejimində identifikasiya olunur.

Bu metodoloji çərçivədə EASM (External Attack Surface Management) təşkilatın xarici perimetrindən görünən boşluqları kəşf etməyə fokuslandığı halda, CAASM (Cyber Asset Attack Surface Management) daxili ekosistemin bütövlüyünü və aktivlərin qarşılıqlı əlaqəsini təmin edir. Bu iki yanaşmanın hibrid inteqrasiyası, müəssisənin kiber-müdafiə arxitekturasında tam görünürlük əldə etməsinə imkan verir.

IV. Hücum Səthinin İdarə Olunması və Sıfır Etibar Modelinin İnteqrasiyası

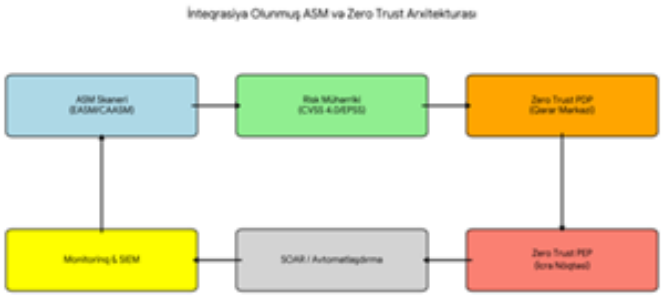
Müasir kiber-təhdid landşaftında təşkilatların qarşılaşdığı ən böyük problem, kəşf edilmiş zəifliklərlə həmin zəifliklərin istismarının qarşısını alan mexanizmlər arasındakı vaxt fərqidir (və ya uçurumdur). Bu bölmədə Hücum Səthinin İdarə Olunması (Attack Surface Management) mühərrikinin Sıfır Etibar (*Zero Trust*) şəbəkə arxitekturası ilə birbaşa əlaqələndirilməsini təmin edən, avtomatlaşdırılmış və reaktiv deyil, proaktiv xarakter daşıyan yeni inteqrasiya modeli təklif olunur.

E. Sıfır Etibar Konseptual Çərçivəsinin Genişləndirilməsi

Sıfır Etibar arxitekturası şəbəkə daxilində və ya xaricində heç bir istifadəçiyə, cihaza və ya tətbiqə avtomatik etibar edilməməsi prinsipini (*"heç vaxt etibar etmə, həmişə yoxla"*) rəhbər tutur. Lakin klassik Zero Trust modelləri adətən istifadəçi kimliyinə (IAM) və cihazın əməliyyat sisteminin vəziyyətinə əsaslanır. Təklif olunan paradiqmada isə HSİO tərəfindən hesablanan dinamik risk qiyməti (R(a)) Zero Trust qərar mexanizminin əsas dəyişəninə çevrilir. Əgər daxili şəbəkədəki hər hansı bir aktivdə (məsələn, bir IoT cihazında və ya Kölgə İT serverində) yeni bir zəiflik (CVE) aşkarlanarsa və EPSS balı bu zəifliyin aktiv istismar ehtimalını yüksək qiymətləndirərsə, cihazın Zero Trust profili dərhal deqradasiyaya uğrayır. Bu yanaşma, hakerin şəbəkə daxilində üfüqi hərəkət (*lateral movement*) etmək imkanlarını sıfıra endirir.

F. İnteqrasiya Edilmiş Sistemin Arxitekturası və İş Prinsipi

Təklif olunan sistem arxitekturası bir-biri ilə API vasitəsilə sinxronizasiya olunan, məlumatın kəşfindən tutmuş insidentin izolyasiyasına qədər bütün həyat dövrünü əhatə edən fundamental təbəqələrdən ibarətdir. (Şəkil 1)



Şəkil 1. Hücum səthinin idarə olunması və Sıfır Etibar arxitekturasının inteqrasiyasının funksional sxemi

Şəkil 1-də göstərilən arxitektura modeli klassik reaktiv müdafiədən fərqli olaraq, qapalı dövrəli bir sistemdir. Proses yeni aktivin aşkarlanması ilə başlayır, riyazi model vasitəsilə risk qiymətləndirilməsinə keçid edir və Sıfır Etibar arxitekturasının vasitəsilə icra (bloklama/izolyasiya) mərhələsi yekunlaşır. Bu model, xüsusilə Kölgə İT resurslarının yaratdığı "görünməzlik" problemini aradan qaldıraraq, təşkilatın hücum səthini proaktiv şəkildə daraldır. Təqdim olunan sistem arxitekturası təkcə iki texnologiyanın birləşməsi deyil, kibertəhlükəsizlikdə reaktiv müdafiədən proaktiv və adaptiv müdafiəyə keçidi təmin edən kompleks bir ekosistemdir. Bu arxitekturada HSİO skaneri daimi olaraq həm xarici (EASM), həm də daxili (CAASM) mühiti skan edərək yeni aktivləri və ya mövcud aktivlərdəki konfiqurasiya səhvlərini aşkarlayır. Aşkarlanan hər bir məlumat dərhal Risk Qiymətləndirmə Mühərrikinə ötürülür və burada təklif olunan riyazi model əsasında aktivin təhlükə səviyyəsi hesablanır. Əldə olunan qiymət real-vaxt rejimində sıfır etibar arxitekturasının beyni hesab olunan Siyasət Qərar Nöqtəsi (Policy Decision Point) komponentinə inteqrasiya edilir. Əgər aktivin risk balı kritik həddi keçərsə, Siyasət Qərar Nöqtəsi dərhal Siyasət İcra Nöqtəsi (Policy Enforcement Point) vasitəsilə həmin aktivin şəbəkəyə girişini bloklayır və ya əlavə identifikasiya (Çoxfaktorlu autentifikasiya) tələb edir. Bu dövriyyə SOAR vasitəsilə avtomatlaşdırıldığı üçün insidentə reaksiya müddəti saniyələrə qədər azalır və insident ehtimalı minimuma enir.

V. Dinamik Risklərin Kəmiyyət Qiymətləndirilməsi və Riyazi Analiz

Müasir informasiya sistemlərində hər gün minlərlə yeni zəiflik (CVE) aşkarlanır, lakin resursların məhdudluğu bütün

boşluqların eyni vaxtda aradan qaldırılmasını qeyri-mümkün edir. Bu bölmədə subyektiv risk mülahizələrini riyazi indikatorlarla əvəz edən dinamik kəmiyyət qiymətləndirilməsi modeli təqdim olunur.

A. CVSS 4.0 və EPSS Metodologiyalarının Sinergetik Təhlili

Tədqiqatımızda risklərin kəmiyyətcə təhlili üçün CVSS 4.0 (Common Vulnerability Scoring System) və EPSS (Exploit Prediction Scoring System) metodologiyalarının hibrid inteqrasiyası təklif olunur. CVSS 4.0 zəifliyin texniki şiddətini müəyyən etdiyi halda, EPSS həmin zəifliyin yaxın 30 gün ərzində real hücumlarda istismar edilmə ehtimalını hesablayır [2].

B. Təklif olunan riyazi risk modeli

Hücum səthində aşkarlanmış hər bir aktiv üçün yekun risk dərəcəsinin kəmiyyət göstəricisi aşağıdakı tənlik əsasında hesablanır:

$$R_a = \frac{S_1 + S_2}{20} \cdot P \cdot K$$

Burada

S_1-CVSS 4.0 üzrə zəifliyin texniki baza göstəricisidir.

$1 \leq S_1 \leq 10$

S_2-Aktivin yerləşdiyi mühitin təhlükəsizlik konfiqurasiyalarını ifadə edən ətraf mühit əmsalıdır.

$1 \leq S_2 \leq 10$

P-Zəifliyin real dünyada istismar edilmə ehtimalıdır.

$0 \leq P \leq 1$

K-Aktivin təşkilat üçün kritikliyini ifadə edən çəki əmsalıdır.

$0 \leq K \leq 1$

C. Kəmiyyət Analizinin Praktiki Təsiri

Təklif olunan model vasitəsilə risklərin kəmiyyətcə qiymətləndirilməsi, "False Positive" xəbərdarlıqların sayını minimuma endirir. Bu yanaşma, Sıfır Etibar mühərrikinə yalnız real təhlükə yaradan aktivləri izolyasiya etmək imkanı verir və kibertəhlükəsizlik layihə meneceri üçün qərarvermə prosesini optimallaşdırır.

VI. Real Praktiki Hücum Ssenarisi və Hücum Səthinin Kiberhücumların Simulyasiyası Baxımından Kəşkiyyatı

Müasir kiberhücumlar getdikcə daha çox təşkilatların idarə olunmayan və görünməyən hücum səthinə yönəlir. Xüsusilə EASM (External Attack Surface Management-Xarici Hücum Səthinin İdarə Olunması) və CAASM (Cyber Asset Attack Surface Management-Kiber Aktiv Hücum Səthinin İdarə Olunması) mexanizmlərinin tətbiq olunmadığı mühitlərdə Kölgə İT (Shadow IT) aktivləri haker üçün ilkin giriş nöqtəsi rolunu oynayır. Bu bölmədə hücum ssenarisi MITRE ATT&CK çərçivəsinə uyğun şəkildə təhlil edilir və əvvəlki bölmədə təklif olunan riyazi risk modelinin praktiki təsdiqi göstərilir.

A. Passiv kəşfiyyat və hücum səthinin aşkarlanması

Haker ilkin mərhələdə OSINT (Open-Source Intelligence-Açıq Mənbəli Kəşfiyyat) və passiv kəşfiyyat üsullarından istifadə edərək təşkilatın hücum səthini müəyyən edir [3]. Bu mərhələ EASM sistemlərinin funksionallığı ilə tam paralellik təşkil edir; fərq isə ondadır ki, EASM bu prosesi müdafiə tərəfində və davamlı, pentester (penetration tester-kiberhücumların simulyasiyası üzrə mütəxəssis/testçi) isə hücum tərəfində və epizodik olaraq həyata keçirir.

Praktikada istifadə olunan əsas alətlər və metodlar aşağıdakılardır:

- Shodan və Censys-internetə açıq portların, banner məlumatlarının və zəif konfiqurasiya olunmuş xidmətlərin axtarışı üçün ixtisaslaşmış axtarış mühərrikləri;
- Subfinder, Amass, Assetfinder-subdomain enumeration (subdomenlərin sadalanması) alətləri; unudulmuş və qeydiyyatdan kənar subdomenləri (məsələn, dev.example.az, legacy-api.example.az) aşkarlayır;
- Sertifikat Şəffaflığı (Certificate Transparency) logları-crt.sh kimi xidmətlər vasitəsilə təşkilatın bütün SSL sertifikatlarının izlənilməsi və kölgə aktivlərin müəyyən edilməsi.

Aşkarlanan tipik aktivlərə daxildir: unudulmuş subdomenlər və köhnə xidmətlər; açıq portlar və yanlış konfiqurasiya olunmuş serverlər; exposed API endpoint-lər (açıq qalmış API endpoint-lər); bulud (Cloud) mühitlərində yanlış paylaşılmış resurslar (məsələn, ictimai S3 bucket-ləri). EASM-in olmaması halında bu aktivlər təşkilat tərəfindən qeydə alınmır və inventarlaşdırılmır, bu da hücum səthinin faktiki ölçüsünü gizlədir.

B. Zəifliklərin identifikasiyası və prioritetləşdirilməsi

Aşkarlanan aktivlər üzərində zəiflik analizi (vulnerability assessment) aparılır və bu mərhələdə aşağıdakı standartlardan istifadə olunur:

- CVE (Common Vulnerabilities and Exposures)-zəifliyin beynəlxalq identifikasiya kataloqu;
- CVSS 4.0 (Common Vulnerability Scoring System)-texniki ciddilik səviyyəsinin qiymətləndirilməsi;
- EPSS (Exploit Prediction Scoring System)-exploit (istismar) olunma ehtimalının proqnozlaşdırılması.

Praktiki müşahidələr göstərir ki, yüksək CVSS balına malik bütün zəifliklər real hücum üçün eyni dərəcədə prioritet daşımır. Bu fərqi iki nümunəvi hal əyani şəkildə nümayiş etdirir: birinci halda CVSS bal 9.8, EPSS isə 0.01 təşkil edir-yəni texniki ciddilik yüksək olsa da, real istismar ehtimalı aşağıdır; ikinci halda CVSS 7.5, EPSS isə 0.85-dir-orta texniki ciddiliyə baxmayaraq, zəiflik aktiv olaraq istismar olunur. Bu nümunələr təklif olunan R(a) modelində T(a) faktorunun (təhdid kəşfiyyatı) daxil edilməsinin real hücum ehtimalını daha dəqiq əks etdirdiyini və klassik yalnız CVSS-ə əsaslanan yanaşmadan üstün olduğunu təsdiqləyir.

C. *İlkin giriş (Initial Access)*

Haker aşağıdakı üsullarla sistemə daxil olur:

- köhnə proqram təminatında (CMS, web framework, VPN gateway) məlum CVE exploit-lərinin tətbiqi;
- default (standart) və ya zəif parolların istifadəsi;
- açıq qalan administrator interfeyslərinin (məsələn, phpMyAdmin, cPanel, Jenkins konsolu) istismarı;
- API autentifikasiya boşluqları (broken authentication və açıq API açarları) vasitəsilə daxilolma.

EASM və CAASM tətbiq olunmadıqda bu aktivlər nəzarətsiz qaldığı üçün exploit prosesi minimal səylə həyata keçirilir.

D. İmtiyazların yüksəldilməsi və üfüqi (lateral) hərəkət

İlkin giriş əldə edildikdən sonra hücumun əsas mərhələsi başlayır. Privilege Escalation (İmtiyazların,səlahiyyətlərin yüksəldilməsi) mərhələsində haker adi istifadəçi səlahiyyətlərindən administrator və ya root səlahiyyətlərinə keçməyə çalışır. Bu mərhələdə LinPEAS, WinPEAS və ya PowerUp kimi avtomatlaşdırılmış skriptlərdən istifadə olunur. İstismar olunan əsas boşluqlar bunlardır: səhv konfiqurasiya olunmuş servis hesabları və SUID binary-lər; köhnə kernel versiyaları və lokal CVE-lər; token və credential (etimadnamə) oğurluğu (məsələn, Mimikatz vasitəsilə).

Lateral Movement (Üfüqi Hərəkət) mərhələsində isə haker daxili şəbəkədə bir sistemdən digərinə keçir. Bu mərhələdə əsasən SMB (Server Message Block), RDP (Remote Desktop Protocol) və SSH (Secure Shell) protokolları vasitəsilə yayılma; Pass-the-Hash və Pass-the-Ticket hücumları; BloodHound və CrackMapExec alətləri ilə Active Directory mühitində domen administratoru hesablarına doğru hərəkət; ortaq istifadə olunan etimadnamələrin (shared credentials) sui-istifadəsi metodlarından istifadə olunur.

Sıfır Etibar modelinin tətbiq edilmədiyi mühitlərdə bu cür təhlükəsizlik zəifliklərı daha asan şəkildə istismar edilə bilir. Klassik perimetr əsaslı təhlükəsizlik yanaşması-yəni "xarici sərt, daxili yumşaq" (hard exterior, soft interior) paradiqması-daxili şəbəkə resurslarını a priori etibarlı hesab etdiyi üçün daxilolma sonrası fəaliyyətlərin kifayət qədər məhdudlaşdırılmamasına səbəb olur. Nəticədə, hücum edən tərəf ilkin giriş əldə etdikdən sonra üfüqi hərəkət (lateral movement) vasitəsilə şəbəkə daxilində aşkarlanmadan genişlənə və sistem üzərində nəzarət səviyyəsini artıra bilir.

E. *Aşkarlanma və gecikmiş reaksiya problemi*

SOAR (Security Orchestration, Automation and Response-Təhlükəsizliyin Orkestrasiyası, Avtomatlaşdırılması və Reaksiyası) və XDR (Extended Detection and Response-Genişləndirilmiş Aşkarlama və Reaksiya) sistemlərinin olmadığı təşkilatlarda hücum daha dərinləşir. Belə mühitlərdə insidentlər SIEM (Security Information and Event Management) loglarında telemetriya səs-küyü içində itir və avtomatik korrelyasiya mexanizmi olmadığı üçün əlaqələndirilmir; MTTD (Mean Time To Detect-aşkarlamaya qədər orta müddət) günlər və ya həftələrlə ölçülür; MTTR (Mean Time To Respond-reaksiyaya qədər orta müddət) qeyri-effektiv şəkildə uzanır. Nəticədə haker persistence (sistemdə davamlılıq) yaratmaq, məlumat eksfiltrasiyası və ya ransomware (zərərli kriptovirus proqramı) yerləşdirmək üçün kifayət qədər vaxt qazanır.

F. *HSİO və Sıfır Etibar inteqrasiyasının hücum zəncirini qırma nöqtələri*

Təklif olunan inteqrasiya olunmuş model bu hücum zəncirini bir neçə nöqtədə qırır [4]. EASM görünməyən və kölgədə qalan aktivləri aşkarlayaraq onları monitorinq sahəsinə daxil edir; CAASM bütün daxili və xarici aktivləri vahid inventarda birləşdirir; Risk Qiymətləndirmə Mühərriki R(a) modeli vasitəsilə CVSS, EPSS və biznes təsiri faktorlarına əsasən prioritetləşdirmə aparır; Zero Trust arxitekturasının Siyasət Qərar Nöqtəsi (Policy Decision Point) və Siyasət İcra Nöqtəsi (Policy Enforcement Point) komponentləri risk əsaslı dinamik giriş nəzarəti tətbiq edir və mikroseqmentasiya prinsipi ilə üfüqi hərəkəti (lateral movement) məhdudlaşdırır; SOAR və XDR sistemləri isə avtomatlaşdırılmış reaksiya ssenariləri-playbook-lar (insident zamanı atılacaq addımların əvvəlcədən hazırlanmış rəqəmsal planı) vasitəsilə insidentə cavab müddətini (MTTR) dəqiqələrə endirir [5].

Nəticədə ilkin giriş mərhələsi əhəmiyyətli dərəcədə çətinləşir; səlahiyyət artırılması (privilege escalation) və üfüqi hərəkət (lateral movement) məhdudlaşdırılır; hücum erkən mərhələdə aşkarlanır və bloklanır; rəqəmsal kriminalistika üçün lazım olan sübut bazası avtomatik formalaşır. Bu yanaşma həm praktiki, həm də riyazi baxımdan modelin effektivliyini təsdiqləyir.

VII. KİBERTƏHLÜKƏSİZLİK LAYİHƏLƏRİNİN İDARƏ OLUNMASINDA HÜCUM SƏTHİNİN İDARƏ OLUNMASININ ROLU

Müasir kibertəhlükəsizlik yanaşmaları yalnız texnoloji deyil, həm də idarəetmə və təşkilati aspektləri əhatə edir. Empirik müşahidələr göstərir ki, kibertəhlükəsizlik layihələrinin uğursuzluğunun fundamental səbəbi texnologiyanın özü deyil, vəzifə bölgüsünün qeyri-müəyyənliyi, məsuliyyət sahələrinin kəsişməməsi və ölçülə bilən performans göstəricilərinin olmamasıdır. Bu səbəbdən HSİO-ın effektiv tətbiqi onu bir texnologiya kimi deyil, kompleks layihə kimi idarə etməyi tələb edir.

A. *Hücum Səthinin İdarə Olunmasının layihə kimi qurulması*

HSİO tətbiqi Layihə İdarəetmə Bilik Bazası (Project Management Body of Knowledge) metodologiyasına əsasən beş klassik mərhələdə həyata keçirilir: təşəbbüs (Initiating), planlaşdırma (Planning), icra (Executing), monitorinq və nəzarət (Monitoring & Controlling), bağlanma (Closing). Lakin HSİO-ın dinamik təbiəti-yəni hücum səthinin daimi dəyişməsi-Agile/Scrum yanaşmasının elementlərinin də inteqrasiyasını tələb edir. Praktikada hibrid model daha effektivdir: strateji səviyyədə PMBOK çərçivəsi (məqsəd, büdcə, maraqlı tərəflər (stakeholders), risk reyestri), əməliyyat səviyyəsində isə Agile sprintləri (hər iki həftədə bir aşkar edilmiş aktivlərin və zəifliklərin emalı) tətbiq olunur. HSİO tətbiqinin əsas mərhələləri aktivlərin identifikasiyası və inventarlaşdırılması, risklərin qiymətləndirilməsi və prioritetləşdirilməsi, düzəliş və zəifliklərin aradan qaldırılması (remediation), eləcə də davamlı monitorinq və təkmilləşdirmədir. Layihənin uğursuzluq

risklərinə təşkilati hazırlıqsızlıq, maraqlı tərəflərin dəstəyinin olmaması, aktiv sahibliyinin müəyyən edilməməsi və HSİO-ın "bir dəfəlik layihə" kimi qəbul edilməsi (halbuki o, davamlı bir prosesdir) daxildir. (Cədvəl I)

B. *RACI matrisi və məsuliyyət bölgüsü*

HSİO proseslərində ən çox rast gəlinən problem məsuliyyət boşluğudur-yəni, aşkar edilən bir zəifliyin kim tərəfindən düzəldiləcəyinin müəyyən olmaması. RACI (Responsible, Accountable, Consulted, Informed) matrisi bu problemin sistematik həllini təmin edir. (Cədvəl I)

CƏDVƏL I. HSİO PROSESLƏRİNDƏ RACI MƏSULİYYƏT MATRİSİ

Proses	**SOC /PT**	**CISO ofisi**	**Layihə meneceri**	**Sistem sahibi**	**İT əmə-liyyat**
Aktivlərin aşkarlanması (EASM/CAASM)	R	A	C	I	C
Risk qiymətləndirilməsinin hesablanması	R	A	C	I	I
Düzəlişin planlaşdırılması	C	A	R	C	I
Düzəlişin tətbiqi	I	A	C	R	R
İnsidentə reaksiya	R	A	C	C	C
Hesabatlılıq və metriklər	C	A	R	I	I

Rolların interpretasiyası aşağıdakı kimidir: Responsible (R)-Məsul, yəni SOC komandası və pentesterlər kimi işi birbaşa icra edənlər; Accountable (A)-Cavabdeh, yəni CISO (Chief Information Security Officer-Baş İnformasiya Təhlükəsizliyi Direktoru) kimi son nəticəyə cavabdeh olan tək şəxs; Consulted (C)- Məsləhətçi, yəni sistem administratorları və DevSecOps, DevOps mühəndisləri kimi qərar verilməzdən əvvəl rəyi alınanlar; Informed (I)-Məlumatlandırılan, yəni biznes rəhbərliyi və digər maraqlı tərəflər kimi nəticə barədə xəbərdar edilənlər.

Bu bölgü olmadıqda tipik bir təşkilatda baş verən problemlər ardıcıllığı belə formalaşır: SOC və ya Pentesting komandası zəifliyi aşkarlayır, lakin İT əməliyyat komandası onun prioritet olduğunu qəbul etmir; sistem sahibi mövcudluq pozulması qorxusu ilə düzəlişi gecikdirir; CISO isə yalnız insident baş verdikdən sonra məlumatlandırılır. Nəticədə zəifliklər sahibsiz qalır, reaksiya gecikir və risklər sistematik şəkildə idarə olunmur.

C. *Risk modelinin layihə idarəetməsinə inteqrasiyası*

Təklif olunan R(a) modeli yalnız texniki bir formula deyil, eyni zamanda layihə idarəetməsində istifadə olunan risk reyestrinin (Risk Register) kəmiyyət əsasını təşkil edə bilər. Klassik risk reyestrində hər risk üçün ehtimal və təsir subyektiv olaraq 1-5 şkalası ilə qiymətləndirilir. R(a) modeli bu subyektivliyi aradan qaldıraraq ehtimal komponentini EPSS (T(a) faktoru) vasitəsilə obyektiv kəmiyyətləndirir, texniki təsir komponentini CVSS 4.0 (V(a)) vasitəsilə standartlaşdırır, biznes təsir komponentini isə FAIR (Factor Analysis of Information Risk) metodologiyası ilə (I(a)) maliyyə dəyərinə çevirir.

Bu inteqrasiya layihə menecerinə həm texniki komandaya, həm də yüksək rəhbərliyə eyni dildə danışmaq imkanı verir: texniki komanda CVSS-i, rəhbərlik isə manatla (maddi ziyanla) ifadə olunan potensial itkini görür. Praktiki tətbiq sahələrinə risk reyestrində zəifliklərin obyektiv prioritetləşdirilməsi, SLA (Service Level Agreement-Xidmət Səviyyəsi Müqaviləsi) müddətlərinin risk qiymətinə görə müəyyən edilməsi (məsələn, R(a) > 8.0 üçün 72 saat), eləcə də resursların və büdcənin risk əsaslı bölüşdürülməsi daxildir.

D. *KPI və performans metrikləri*

HSİO layihəsinin effektivliyi aşağıdakı kəmiyyət göstəriciləri ilə ölçülür:

- MTTD (Mean Time To Detect)-yeni aktivin və ya zəifliyin aşkar edilmə müddəti; effektiv HSİO tətbiqi MTTD-ni günlərdən saatlara endirir;
- MTTR (Mean Time To Respond/Remediate)-insidentə və ya zəifliyə reaksiya müddəti; SOAR inteqrasiyası ilə bu göstərici dəqiqələrə qədər azalır;
- Asset Coverage (Aktiv əhatə dairəsi, %)-bilinən aktivlərin ümumi aktivlərə nisbəti; sənaye standartı kimi 95%-dən yuxarı hədəf qoyulur;
- Shadow IT Ratio (Kölgə İT nisbəti)-aşkar edilmiş kölgə aktivlərin ümumi aktivlərə nisbəti;
- Average R(a) (Orta risk qiyməti)-təşkilatın ümumi risk profilinin zaman içində dəyişməsini izləyən aqreqat göstərici;
- SLA compliance rate (SLA-ya uyğunluq faizi)-risk səviyyəsinə görə müəyyən edilmiş müddətlərdə tamamlanan düzəlişlərin faizi.

Bu metriklər həm texniki komandaya, həm də biznes rəhbərliyinə təhlükəsizlik səviyyəsini obyektiv qiymətləndirmək imkanı verir.

E. Kölgə İnformasiya Texnologiyasının yaranma səbəbləri: idarəetmə perspektivi

Kölgə İT yalnız texniki nəzarətsizliyin nəticəsi deyil, fundamental olaraq idarəetmə və təşkilati mədəniyyət problemidir. Praktikada onun yaranma səbəblərinə İT proseslərinin ləngliyi və bürokratik gecikmələr (İT departamentinin yeni xidmət təminatı prosesi həftələrlə uzandıqda biznes vahidləri öz büdcəsi ilə SaaS xidmətləri əldə edir); mərkəzləşdirilməmiş satınalma siyasəti (departamentlərin müstəqil olaraq texnologiya seçməsi və İT-yə bildirməməsi); istifadəçilərin rahatlıq üstünlüyü (işçilərin icazəsiz tətbiqlərə müraciət etməsi); uzaqdan iş və BYOD (Bring Your Own Device-Şəxsi Cihazını Gətir) mədəniyyəti; birləşmə və satınalma (M&A) prosesləri zamanı yeni şirkətlərin İT inventarının tam inteqrasiya edilməməsi; köhnə layihələrdən qalan və deaktiv edilməyən test serverləri, subdomenlər və API-lər; eləcə də mərkəzləşdirilmiş aktiv qeydiyyatı prosedurunun olmaması daxildir.

Yalnız texniki HSİO aləti ilə bu problemin həlli mümkün deyil-paralel olaraq texnologiya əldə etmə siyasəti, işçi maarifləndirilməsi və mərkəzləşdirilmiş aktiv qeydiyyatı proseduru tətbiq edilməlidir. Bu, NIST CSF (Cybersecurity Framework) 2.0-ın yeni İdarəetmə funksiyasının praktiki tətbiqidir.

F. Hücum Səthinin İdarə Olunması və düzgün idarəetmə modelinin olmamasının nəticələri

HSİO tətbiq olunmadıqda və ya layihə idarəetmə çərçivəsi qurulmadıqda təşkilat aşağıdakı sistemli risklərlə üzləşir: hücum səthi nəzarətsiz şəkildə böyüyür və faktiki ölçüsü məlum olmur; risklər subyektiv və qeyri-obyektiv qiymətləndirilir; zəifliklər sahibsiz qalır və məsuliyyət bölgüsü qeyri-müəyyən olur; insidentlər gec aşkarlanır (yüksək MTTD) və reaksiya gecikir (yüksək MTTR); kölgə İT aktivləri monitorinq olunmur və yüksək risk yaradır; rəqəmsal kriminalistika üçün lazım olan sübut bazası zəifləyir, çünki aktiv inventarı və tarixçəsi qeydə alınmır; tənzimləyici tələblərə (məsələn, GDPR, ISO 27001) uyğunluq pozulur.

G. *Kibertəhlükəsizlik layihə menecerinin Hücum Səthinin İdarə Olunması ekosistemində rolu*

Kibertəhlükəsizlik layihə meneceri (Cybersecurity Project Manager) HSİO tətbiqində körpü rolunu oynayır: texniki komanda (SOC, pentester, mühəndislər) ilə biznes rəhbərliyi arasında kommunikasiyanı təmin edir; R(a) risk qiymətlərini biznes risk dilinə tərcümə edir; düzəliş tapşırıqlarını sistem sahibləri arasında paylaşdırır və SLA-ya uyğunluğu izləyir; maraqlı tərəflərin gözləntilərini idarə edir və layihənin davamlı maliyyələşdirilməsini təmin edir; uyğunluq (compliance) tələblərinin layihə daxilində izlənməsini təşkil edir.

Beləliklə, HSİO uğurunun düsturu sadəcə "Texnologiya × Riyazi Model" kimi deyil, "Texnologiya × Riyazi Model × İdarəetmə Çərçivəsi" kimi ifadə oluna bilər. Bu üçölçülü yanaşma kibertəhlükəsizliyin müasir paradiqmasında nəzəri modelin praktiki effektivliyinin əsas şərtidir.

NƏTİCƏ

Tədqiqat işində müasir kiber-təhdid mühitinin ən kritik problemlərindən biri olan idarəolunmayan hücum səthi və Kölgə İT resurslarının yaratdığı risklər kompleks şəkildə analiz edilmişdir. Ənənəvi perimetr əsaslı müdafiə strategiyalarının effektivliyini itirdiyi rəqəmsal transformasiya dövründə, Hücum Səthinin İdarə Olunması ekosisteminin Sıfır Etibar (Zero Trust) arxitekturası ilə sinergetik inteqrasiyasını təmin edən proaktiv və adaptiv bir model təklif olunmuşdur.

Təqdim olunan modelin əsas elmi və praktiki töhfələri aşağıdakılardır:

Dinamik Kəmiyyət Qiymətləndirilməsi: Müəssisənin həm daxili (CAASM), həm də xarici (EASM) aktivlərinin kəşfiyyatı əsasında, zəifliklər CVSS 4.0, EPSS və FAIR metodologiyalarının hibrid kombinasiyasından ibarət riyazi risk modeli vasitəsilə kəmiyyətcə qiymətləndirilmişdir.

Avtomatlaşdırılmış İcra Mexanizmi: Hesablanmış risk dərəcələri Siyasət Qərar və İcra Nöqtələrinə (PDP/PEP) inteqrasiya edilərək, SOAR texnologiyasının köməyi ilə insidentə reaksiya müddəti saniyələrə endirilmiş və hakerlərin üfüqi hərəkət (lateral movement) imkanları effektiv şəkildə bloklanmışdır.

İdarəetmə Çərçivəsinin Tətbiqi: Kibertəhlükəsizliyin təkcə texnoloji aspektləri ilə kifayətlənməyərək, layihə idarəetməsi kontekstində RACI məsuliyyət matrisi və yeni kəmiyyət göstəriciləri (MTTD, MTTR, Kölgə İT nisbəti) işlənib hazırlanmışdır. Bu isə kibertəhlükəsizlik layihə menecerlərinə subyektiv risk mülahizələrini obyektiv metriklərə çevirmək imkanı yaradır.

Nəticə etibarilə, bu tədqiqat işi sadəcə texnoloji və ya riyazi bir həll deyil, kibertəhlükəsizliyin müasir paradiqmasında "Texnologiya × Riyazi Model × İdarəetmə Çərçivəsi" yanaşmasını reallaşdıran kompleks bir ekosistemdir. Bu üçölçülü yanaşmanın tətbiqi rəqəmsal aktivlərin tam görünürlüyünü bərpa edir, ISO/IEC 27001 kimi normativ-hüquqi çərçivələrə uyğunluğu təmin edir və milli kiber-dayanıqlıq strategiyalarının formalaşdırılmasına mühüm töhfə verir.

ƏDƏBİYYAT

[1] NIST, "NIST Special Publication 800-207: Zero Trust Architecture," National Institute of Standards and Technology, Gaithersburg, MD, 2020.

[2] FIRST.org, "Common Vulnerability Scoring System v4.0 Specification," Forum of Incident Response and Security Teams, 2023: https://www.first.org/cvss/v4.0/specification-document

[3] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, "Exploit Prediction Scoring System (EPSS)," Digital Threats: Research and Practice, vol. 2, no. 3, pp. 1–17, Jul. 2021.

[4] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, pp. 273–284, 2002.

[5] J. Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, 2010.

Attack Surface Management in Information Systems and Integration of Modern Cybersecurity Models

Ravan Rasulzada[1], Lamiya Najafova[2]
[1]Azerbaijan Technical University, Baku, Azerbaijan
[2]Institute of Mathematics, Baku, Azerbaijan
[1]ravanrasulzada@gmail.com, [2]najafova.lamiya@gmail.com

Abstract- The article investigates the integrated application of Attack Surface Management and Zero Trust models. The study proposes a proactive model based on CVSS 4.0, EPSS, and FAIR methodologies for asset discovery, monitoring, and quantitative risk assessment. The proposed approach utilizes a novel mathematical model and system architecture, grounded in modern risk assessment methodologies such as CVSS 4.0, EPSS and FAIR.

Keywords- attack surface management; zero trust; cybersecurity risks; shadow information technology; risk assessment.