Proqram Sistemlərində Kiberinsidentlərin Qarşısının Alınması üçün Aktiv və Proaktiv Mexanizmlərin Tətbiqi

Tofiq Kazımov[1], Nəzakət Məlikova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*tofig@mail.ru*, [2]*naranara_68@mail.ru*

***Xülasə*— Rəqəmsal texnologiyaların sürətli inkişafı, Əşyaların İnterneti , bulud texnologiyaları və paylanmış sistemlərin geniş tətbiqi kiberhücumların sayını və mürəkkəbliyini artırmışdır. Məqalədə müasir proqram sistemlərində kibertəhlükəsizliyin əsas problemləri və onların həlli yolları təhlil olunmuş, kibertəhdidlərin əsas xüsusiyyətləri, onların yaranma səbəbləri araşdırılmış, kibertəhlükəsizliyin təmin olunmasında aktiv və proaktiv yanaşmaların rolu müqayisəli şəkildə təhlil edilmişdir. Eyni zamanda, çoxqatlı müdafiə modelinin tətbiqinin zəruriliyi əsaslandırılmışdır.**

Açar sözlər— kibertəhlükəsizlik; kiberhücumlar; proaktiv təhlükəsizlik; reaktiv təhlükəsizlik; çoxqatlı müdafiə.

I. GİRİŞ

Son illərdə kiberhücumların intensivliyinin və mürəkkəbliyinin artması müasir cəmiyyətin rəqəmsal texnologiyalarla sıx inteqrasiyası ilə əlaqəlidir. Kibercinayətkarlıq müasir təhlükə mühitinin əsas komponentlərindən biri olmaqla dövlət qurumları, korporativ strukturlar və fərdi istifadəçilər üçün ciddi risklər yaradır ki, bu da çox böyük maddi itkilərlə nəticələnə bilir.

Əşyaların İnternetinin (İoT) geniş tətbiqi və qlobal şəbəkə mühitində təhlükələrin intensivləşməsi son illərdə kiberhücumların sayının artmasını şərtləndirmişdir. Kiberhücumlar müxtəlif məqsədlərə yönələ bilər: məxfi informasiyanın qanunsuz əldə edilməsi, kritik informasiya infrastrukturunun sıradan çıxardılması, maliyyə fırıldaqçılığı və s.

Kibertəhdidlərin aktuallığı həm hücum edən tərəflərin, həm də müdafiə mexanizmlərini formalaşdıran subyektlərin istifadə etdiyi texnologiyaların dinamik inkişafı ilə əlaqədardır. Bu hücumların reallaşdırılma üsulları getdikcə daha çoxşaxəli və kompleks xarakteri alır: bunlara fişinq, DDoS hücum növləri və proqram təminatındakı zəifliklərin istismarı kimi qabaqcıl texniki metodları əhatə edir [1].

Əsas problem ondan ibarətdir ki, bir çox təşkilat və istifadəçi kiberhücumlardan kifayət qədər qorunmur. Bu vəziyyət yalnız potensial təhdidlər barədə məlumatın məhdudluğu ilə deyil, eyni zamanda sürətlə dəyişən və daim yenilənən hücum metodlarına qarşı effektiv müdafiə mexanizmlərinin formalaşdırılmasında çətinliklərlə də izah olunur. Nəticə etibarilə, mövcud boşluqlar kiberinsidentlərin başvermə ehtimalını artırır və onların təsir miqyasını genişləndirir [2].

II. KİBERTƏHLÜKƏSİZLİYİN ƏSAS PROBLEMLƏRİ

Kibertəhlükəsizliyin əsas problemləri müasir rəqəmsal mühitdə həm texniki, həm təşkilati, həm də insan amilləri ilə sıx bağlıdır. Əsas problemlər aşağıdakılardır [3]:

A *Kibertəhdidlərin sürətlə artması və mürəkkəbləşməsi*

Hakerlər və kiberqruplar getdikcə daha inkişaf etmiş üsullardan istifadə edir. Süni intellekt, avtomatlaşdırılmış hücumlar və yeni zərərli proqramlar (malware) təhlükələri daha çətin aşkar olunan edir.

B *Hücum səthinin genişlənməsi*

Bulud texnologiyaları, IoT cihazları (ağıllı qurğular) və uzaqdan iş modelləri sistemlərə giriş nöqtələrini artırır. Bu amil hücum ehtimalının artmasına səbəb olur.

C *İnsan amili*

İstifadəçilərin səhvləri – zəif parollar, fişinq (phishing) linklərinə klikləmə, təhlükəsizlik qaydalarına əməl etməmək – kibertəhlükəsizliyin ən böyük problemlərindən biridir.

D *Kadr çatışmazlığı*

Təcrübəli kibertəhlükəsizlik mütəxəssislərinin azlığı təşkilatların müdafiəsini zəiflədir və riskləri artırır.

E *Köhnəlmiş sistemlər və proqramlar*

Bir çox təşkilatlar yenilənməyən (outdated) proqram təminatından istifadə edir. Bu sistemlərdə məlum zəifliklər olur və hücumçular üçün asan hədəfə çevrilir.

F *Zəif təhlükəsizlik strategiyası*

Bəzi təşkilatlar yalnız insident baş verdikdən sonra reaksiya verir (reaktiv yanaşma) və qabaqlayıcı tədbirlərə kifayət qədər diqqət ayırmır.

G *Sürətlə dəyişən texnologiyalar*

Yeni texnologiyalar (Sİ, blockchain və s.) inkişaf etdikcə, onların təhlükəsizlik problemləri də paralel olaraq yaranır və bəzən bu risklər əvvəlcədən tam bilinmir.

H *Hücumların aşkarlanmasının çətinliyi*

Bəzi hücumlar uzun müddət gizli qalır (advanced persistent threats – APT). Bu da onların vaxtında aşkarlanmasını çətinləşdirir.

III. QANUNVERİCİLİK VƏ UYĞUNLUQ PROBLEMLƏRİ

Təşkilatlar müxtəlif standartlara (ISO, GDPR və s.)

DOI: 10.25045/forensic.gov.2026.13

uyğunlaşmaqda çətinlik çəkir ki, bu da həm hüquqi, həm də əməliyyat risklərinin artmasına səbəb olur. Belə şəraitdə təşkilatların kibertəhlükəsizlik strategiyalarında yalnız normativ tələblərə uyğunlaşma deyil, həm də effektiv müdafiə mexanizmlərinin tətbiqi xüsusi əhəmiyyət kəsb edir. Bu müdafiə yanaşmaları içərisində reaktiv və aktiv mexanizmlər mühüm yer tutur.

Yuxarıda qeyd olunan problemlər, xüsusilə uzun müddət gizli qalan APT hücumları və qanunvericiliklə bağlı uyğunluq çətinlikləri, müasir kibertəhlükəsizlik yanaşmalarının daha sistemli və inteqrasiya olunmuş şəkildə qurulmasını zəruri edir. Bu baxımdan, kibersuverenliyin təmin olunması üçün həm proaktiv (hücumlardan əvvəl), həm də aktiv (hücum zamanı) mexanizmlərin paralel tətbiqi vacibdir. Şəkil 1 bu yanaşmanın strukturunu və onun nəticəsi kimi formalaşan dayanıqlılıq modelini əks etdirir."

Şəkil 1. Proqram sistemlərində kibertəhlükəsizliyin təmin olunmasının funksional sxemi

IV. AKTİV MEXANİZMLƏRİN XÜSUSİYYƏTLƏRİ

Aktiv mexanizmlər hücum baş verdiyi anda və ya dərhal sonra işə düşərək onun təsirini minimuma endirməyə yönəlmiş müdafiə vasitələridir.

Bu mexanizmlərin əsas məqsədi hücumun yayılmasının qarşısını almaq və sistemin normal fəaliyyətini qorumaqdır.

Aktiv mexanizm:

- Hücum səthinin azaldılması
- Erkən aşkarlama və cavab
- Dayanıqlı təhlükəsizlik
- Zero-day risklərinin azalması
- ISO 27001, NIST uyğunluğu

Bu mexanizmlərə aiddir [4]:

- Hücumun aşkarlanması və qarşısının alınması (Intrusion Detection System – IDS);
- Şübhəli trafiki və davranışları aşkarlayaraq bloklayır (Intrusion Prevention System – IPS);
- Antivirus;
- Yalnız cihaz səviyyəsində qoruma (Endpoint Detection and Response – EDR) və bütün sistem üzrə qoruma (Extended Detection and Response-XDR) platformaları, Təhlükəsiz İnformasiya və Hadisələrin İdarə Olunması (Security Information and Event Management – SIEM) sistemləri və real-vaxt log monitorinqi;
- İnsidentlərə cavabvermə mexanizmləri;
- Web Application Firewall (WAF)– vebsaytı hücumlardan qoruyan ağıllı filtr rolunu oynayır.

V. PROAKTİV MEXANİZMLƏRİN XÜSUSİYYƏTLƏRİ

Proaktiv mexanizmlər hücumlar baş verməzdən əvvəl risklərin azaldılmasına və zəifliklərin aradan qaldırılmasına yönəlmiş müdafiə mexanizmidir. Bu mexanizm proqram sisteminin təhlükəsizliyini uzunmüddətli təmin edir. Bu mexanizmlərə aiddir:

- Statik və dinamik kod analizi (Static Application Security Testing - SAST/ Dynamic Application Security Testing – DAST)
- Girişə nəzarət siyasətləri (Least privilege. Multi-Factor Authentication – MFA)
- Təhlükəsiz Proqram Təminatının Yaradılmasının Həyat Dövrü (Secure Software Development Lifecycle – SSDLC) PT- nin hazırlanmasının bütün mərhələlərində təhlükəsizliyin əvvəlcədən nəzərə alındığı proaktiv yanaşmadır.
- Təhlükəsizlik maarifləndirmə proqramları

Beləliklə, proaktiv mexanizmlərin tətbiqi təkcə ayrı-ayrı təhlükələrin qarşısını almaqla kifayətlənmir, həm də daha geniş və sistemli müdafiə yanaşmalarının formalaşdırılmasını zəruri edir. Bu baxımdan, müasir kibertəhlükəsizlik strategiyalarında "Defense in Depth" (çoxqatlı müdafiə) yanaşması xüsusi əhəmiyyət kəsb edir və proqram sistemlərində çoxqatlı kibertəhlükəsizlik modelinin əsasını təşkil edir [5].

VI. REAKTİV MEXANİZMLƏR

Reaktiv mexanizmlər kiber təhlükəsizlik strategiyasının "hücumdan sonrakı" (post-incident) mərhələsini əhatə edir. Bu mərhələnin əsas məqsədi baş vermiş insidentin fəsadlarını aradan qaldırmaq və sistemi əvvəlki işlək vəziyyətinə qaytarmaqdır.

Aşağıda reaktiv mexanizmlərin əsas komponentləri və onların funksiyaları haqqında ətraflı məlumat verilmişdir:

1. İnsidentə reaksiya -Hücum aşkar edildikdən dərhal sonra həyata keçirilən ilk addımdır. Bura hücumun yayılmasının qarşısını almaq (lokallaşdırma) və təsirə məruz qalmış sistemlərin izolyasiyası daxildir.

2. Hücumun təhlili və rəqəmsal ekspertiza -Hücumun necə baş verdiyini, hansı boşluqlardan istifadə edildiyini və hansı məlumatların sızdığını anlamaq üçün aparılan araşdırmadır. Bu, gələcəkdə bənzər hücumların qarşısını almaq üçün çox vacibdir.

3.Sistemlərin bərpası - Zərər görmüş faylların, verilənlər bazasının və proqram təminatının ehtiyat nüsxələrdən (backup) istifadə edərək yenidən qurulmasıdır. Bu mərhələdə xidmətlərin minimum vaxt itkisi ilə bərpası prioritet təşkil edir.

4. Dərslər və təkmilləşdirmə -Baş vermiş hadisədən nəticə çıxararaq təhlükəsizlik siyasətlərinə düzəlişlər edilməsidir. Reaktiv mexanizm burada dövrəni tamamlayır və əldə olunan təcrübə Proaktiv mexanizmləri (məsələn, yeni zəiflik analizlərini) gücləndirmək üçün istifadə olunur.

VII. PROQRAM SİSTEMLƏRİNDƏ ÇOXQATLI KİBER-TƏHLÜKƏSİZLİK YANAŞMASI

Defense in Depth (çoxqatlı müdafiə) strategiyası — Proqram sistemlərinin və informasiya resurslarının kiberhücumlara qarşı qorunması üçün bir neçə müstəqil və bir-birini tamamlayan təhlükəsizlik səviyyələrinin (qatlarının) eyni vaxtda tətbiq edildiyi təhlükəsizlik strategiyasıdır. Bu yanaşmada təhlükəsizlik tək bir mexanizmə (məsələn, yalnız firewall və ya yalnız antivirus) əsaslanmır. Əksinə, sistemin müxtəlif hissələrində yerləşdirilmiş müdafiə qatları hücumçunun sistemə daxil olmasını mərhələli şəkildə çətinləşdirir və ya tamamilə mümkünsüz edir.

Defense in Depth strategiyası aşağıdakı əsas funksiyaları yerinə yetirir:

Hücumların qarşısını mərhələli şəkildə alır.

Əgər hücumçu bir təhlükəsizlik qatını keçərsə növbəti qat onu dayandırır və ya hücumun təsirini azaldır.

Sistemin tam sıradan çıxmasının qarşısını alır.

Defense in Depth nə üçün vacibdir?

Defense in Depth — hücumları tək bir nöqtədə deyil, sistemin müxtəlif səviyyələrində aşkar edib qarşısını almağa yönəlmiş çoxqatlı təhlükəsizlik yanaşmasıdır. Bu yanaşma risklərin bölüşdürülməsini təmin edir, ayrı-ayrı zəifliklərin təsirini kompensasiya edir və nəticə etibarilə sistemin ümumi dayanıqlığını artırır.

Belə bir kompleks təhlükəsizlik modelinin effektiv tətbiqi isə yalnız texniki tədbirlərlə məhdudlaşmır, həm də təşkilati və idarəetmə səviyyəsində düzgün strateji yanaşmanın formalaşdırılmasını tələb edir. Bu baxımdan rəhbərlik səviyyəsində qəbul edilən qərarlar həlledici rol oynayır.

NƏTICƏ

Aparılmış tədqiqat göstərir ki, müasir proqram sistemlərində kiberhücumların qarşısının alınması yalnız ayrı-ayrı texniki vasitələrin tətbiqi ilə deyil, aktiv və proaktiv təhlükəsizlik mexanizmlərinin kompleks və inteqrasiya olunmuş şəkildə istifadəsi ilə mümkündür. Rəqəmsal texnologiyaların sürətli inkişafı, bulud əsaslı sistemlərin, IoT mühitlərinin və paylanmış arxitekturaların geniş yayılması kiberhücumların həm miqyasını, həm də mürəkkəbliyini əhəmiyyətli dərəcədə artırmışdır.

Nəticə etibarilə, proqram sistemlərinin kiberdayanıqlığının artırılması üçün təhlükəsizliyin dizayn mərhələsindən başlayaraq istismar mərhələsinədək davamlı şəkildə idarə olunması, eləcə də aktiv və proaktiv təhlükəsizlik mexanizmlərinin balanslı tətbiqi zəruri hesab olunur. Bu yanaşma yalnız mövcud kiberhücumların qarşısının alınmasını deyil, eyni zamanda gələcək potensial təhdidlərə qarşı adaptiv və dayanıqlı müdafiə mühitinin formalaşdırılmasını təmin edir.

Təşkilatlar yalnız aktiv yanaşmaya (insident baş verdikdən sonra reaksiya verməyə) əsaslanmamalıdır. Bunun əvəzinə, proaktiv və reaktiv tədbirləri birlikdə tətbiq edən balanslı strategiya qurulmalıdır. Təhlükəsizlik sadəcə texniki məsələ kimi deyil, strateji biznes prioriteti kimi qəbul edilməlidir və bütün səviyyələrdə investisiya tələb edir. Rəhbərlik təhlükəsizliyin effektivliyini ölçmək üçün aydın göstəricilər müəyyən etməlidir. Bu göstəricilər həm reaktiv ölçüləri (məsələn, insidentin aşkarlanma və cavab müddəti), həm də proaktiv ölçüləri (məsələn, təhlükəsizlik analizindən keçmiş kodun faizi, kritik hissələr üzrə risk analizinin aparılması, zəifliyin aşkar edilməsindən düzəldilməsinə qədər olan vaxt) əhatə etməlidir. Erkən mərhələlərdə təhlükəsizliyə yatırım etmək xüsusilə vacibdir. Araşdırmalar göstərir ki, layihələndirmə mərhələsində təhlükəsizliyə qoyulan 1 dollar sonradan 30–100 dollar qənaət etməyə kömək edir. Buna görə də proaktiv təhlükəsizlik xərc deyil, uzunmüddətli investisiya kimi qiymətləndirilməlidir. Bu, həm maliyyə baxımından sərfəlidir, həm reputasiya risklərini azaldır, həm də qanunvericilik tələblərinə uyğunluğu təmin edir.

Beləliklə, rəhbərlik səviyyəsində qəbul edilən bu strateji yanaşmalar təşkilatlarda təhlükəsizliyin yalnız konseptual deyil, həm də ölçülə bilən və davamlı şəkildə idarə olunan prosesə çevrilməsini təmin edir. Erkən mərhələlərdə təhlükəsizliyə investisiya qoyulmasının effektivliyi də onu göstərir ki, proaktiv yanaşma praktik müstəvidə real nəticələr verir və risklərin minimallaşdırılmasında həlledici rol oynayır.

Bu baxımdan, müəyyən edilmiş strateji prinsiplərin əməli səviyyədə tətbiqi xüsusi əhəmiyyət kəsb edir. Yəni, təşkilatlar yalnız ümumi yanaşmalarla kifayətlənməməli, eyni zamanda proaktiv təhlükəsizliyin konkret texniki və metodoloji mexanizmlər vasitəsilə necə reallaşdırılacağını da müəyyən etməlidirlər.

Proaktiv təhlükəsizlik sisteminin arxitekturası hazırlanarkən risklərin əvvəlcədən analizindən başlamalıdır. Hər yeni layihə və ya mövcud sistemdə ciddi dəyişiklik zamanı memarlar, proqramçılar və təhlükəsizlik mütəxəssisləri birlikdə risklərin (təhdidlərin) qiymətləndirilməsini aparmalıdırlar. Bu analiz nəticələri sənədləşdirilməli və hansı qoruyucu tədbirlərin daha vacib olduğunu müəyyən etmək üçün istifadə olunmalıdır. Təşkilatlar layihələndirmə mərhələsində təhlükəsizlik (Security by Design) prinsipini tətbiq etməlidirlər. Bu o deməkdir ki, təhlükəsizlik tələbləri funksional tələblər qədər vacib sayılmalıdır; sistemdə çoxqatlı müdafiə (defense in depth), minimal səlahiyyət (least privilege), təhlükəsiz dayanma (fail secure) və zero trust kimi prinsiplər tətbiq olunmalıdır; proqramlaşdırmaya başlamazdan əvvəl təhlükəsizlik baxımından arxitektura yoxlanılmalıdır. Təhlükəsizlik sonradan əlavə edilən funksiya deyil, sistemin əsas keyfiyyət tələbi kimi başlanğıcdan inteqrasiya olunmalıdır.

Beləliklə, Security by Design prinsipinin tətbiqi təhlükəsizliyin sistemin ilkin mərhələlərindən etibarən inteqrasiya olunmasını təmin edir və potensial zəifliklərin erkən

aşkarlanmasına imkan yaradır. Lakin bu yanaşmanın davamlı və sistemli şəkildə həyata keçirilməsi üçün təhlükəsizlik tədbirlərinin yalnız arxitektura səviyyəsində deyil, proqram təminatının bütün həyat dövrü boyunca inteqrasiya olunması zəruridir.

Bu baxımdan, təhlükəsizliyin hər mərhələdə təmin olunmasını nəzərdə tutan SSDLC yanaşması xüsusi əhəmiyyət kəsb edir.

Təhlükəsiz Proqram Təminatının Yaradılmasının Həyat Dövrü ilə bağlı tövsiyələr

SSDLC təhlükəsizliyin proqramın bütün inkişaf mərhələlərinə daxil edilməsini nəzərdə tutur: Tələblər mərhələsində – təhlükəsizlik və məxfilik tələbləri müəyyən edilməlidir. Layihələndirmə mərhələsində – risklərin analizi və təhlükəsizlik yönümlü arxitektura hazırlanmalıdır.Proqramlaşdırma mərhələsində – təhlükəsiz kodlaşdırma qaydalarına əməl olunmalı, kod yoxlamaları aparılmalı və statik analiz alətlərindən istifadə edilməlidir.Test mərhələsində – dinamik təhlükəsizlik testləri, penetrasiya testləri və təhlükəsizlik üzrə təkrar testlər həyata keçirilməlidir. Nəticə olaraq, təhlükəsizliyin effektiv təmin olunması üçün təşkilatlar həm qabaqlayıcı (proaktiv), həm də cavabverici (aktiv) yanaşmaları birlikdə və sistemli şəkildə tətbiq etməlidirlər.

Beləliklə, SSDLC yanaşması təhlükəsizliyin proqram təminatının bütün həyat dövrü boyunca sistemli şəkildə təmin olunmasına imkan yaradır və həm proaktiv, həm də aktiv tədbirlərin inteqrasiyasını təmin edən mühüm çərçivə kimi çıxış edir. Bu yanaşma nəticə etibarilə proqram sistemlərinin dayanıqlığını artırır və müasir kibertəhdidlərə qarşı daha effektiv müdafiə mühitinin formalaşmasına şərait yaradır.

ƏDƏBİYYAT

[1] M. A. Ribeiro et al., "Detecting and mitigating DDoS attacks with moving target defense," Computers & Security, 2023. DOI: 10.1016/j.cose.2023.003723

[2] Н. М. Кодацкий, А. С. Мотуз Угрозы кибербезопасности в информационной среде //StudNet. — Т. 5. – №. 1. – С. 633-639, 2022.

[3] И. М. Полухтин Актуальные проблемы кибербезопасности в современном мире //Вестник науки. — Т. 4. – №. 6 (63). – С. 608-612. 2023.

[4] Ерастов Е. Д. Современные проблемы кибербезопасности: вызовы и решения //Вестник науки. – 2024. – Т. 4. – №. 10 (79). – С. 745-749.

[5] W. Villegas-Ch et al., "Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.10778531

Implementation of Active and Proactive Mechanisms for Preventing Cyber Incidents in Software Systems

Tofig Kazimov[1], Nazakat Malikova[2]

[1,2]Institute of Information Technology, Baku, Azerbaijan

[1]*tofig@mail.ru*, [2]*naranara_68@mail.ru*

Abstract- The rapid development of digital technologies, the widespread use of the Internet of Things (IoT), cloud technologies and distributed systems has increased the number and complexity of cyberattacks. The article analyzes the main problems of cybersecurity in modern software systems and their solutions, examines the main characteristics of cyberthreats, the causes of their emergence, and compares the role of active and proactive approaches in ensuring cybersecurity. At the same time, the necessity of applying the Defense in Depth model is justified.

Keywords- cybersecurity; cyberattacks; proactive security; reactive security; Defense in Depth.