PARADIGMA, No.1, 2026, səh.169-173
https://doi.org/10.30546/30015.2026.01.01.2090

KİBERTƏHLÜKƏSİZLİK ÜÇÜN ARXİTEKTURANIN QURULMASI: TƏŞKİLATLARDA SİSTEMLİ VƏ DAYANIQLI YANAŞMA

İ.İ. Seyfullayev, S.T. Əliyeva
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: isa.seyfullayev@student.au.edu.az

Xülasə. Kibertəhlükəsizlik arxitekturasının qurulması təşkilatın informasiya sistemlərini kiber təhdidlərə qarşı davamlı və idarəolunan formada qorumağa yönəlmiş kompleks yanaşmadır. Bu arxitektura risklərin qiymətləndirilməsi, çoxqatlı müdafiə (defense-in-depth), şəbəkə segmentasiyası, identifikasiya və girişlərin idarə edilməsi (IAM), sistem sərtləşdirilməsi (hardening), davamlı monitorinq və insidentlərə cavab mexanizmlərinin inteqrasiyası əsasında formalaşdırılır. Nəticədə hücumların qarşısı alınır, erkən mərhələdə aşkarlanması təmin olunur və insident zamanı xidmətlərin fasiləsizliyi ilə sürətli bərpa imkanları artırılır.

Açar sözlər: Kibertəhlükəsizlik arxitekturası, risk analizi, defense-in-depth, Zero Trust, şəbəkə segmentasiyası, IAM, SIEM/SOC, insident cavabı, hardening, biznes davamlılığı.

Giriş

Müasir dövrdə təşkilatların rəqəmsal transformasiyası ilə paralel olaraq kibertəhlükələr də daha mürəkkəb və çoxşaxəli xarakter almışdır. İnformasiya sistemlərinin genişlənməsi, bulud infrastrukturlarının yayılması, uzaqdan iş modelləri və IoT cihazlarının istifadəsi hücum səthini (attack surface) artırır. Nəticədə təkcə texniki müdafiə tədbirləri ilə kifayətlənmək mümkün deyil, təşkilatlar kompleks kibertəhlükəsizlik arxitekturası formalaşdırmalı, təhlükəsizliyi sistemin bütün qatlarında planlı şəkildə qurmalıdırlar.

Kibertəhlükəsizlik arxitekturası dedikdə, informasiya sistemlərinin məxfiliyini (confidentiality), bütövlüyünü (integrity) və əlçatanlığını (availability) təmin edən texniki, prosedur və təşkilati komponentlərin bir-biri ilə əlaqəli şəkildə dizayn olunması başa düşülür. Arxitekturanın məqsədi təkcə mövcud riskləri azaltmaq deyil, həm də gələcək hücum ssenarilərinə qarşı dayanıqlı mühit formalaşdırmaqdır. Bu baxımdan arxitektura qurmaq hücumların qarşısının alınması, vaxtında aşkarlanması və düzgün cavab vermə mexanizmlərinin birlikdə işlədiyi sistemli yanaşmanı tələb edir.

Arxitekturanın qurulmasının əsas istiqamətləri

1. Tələblərin toplanması və mövcud vəziyyətin təhlili

Arxitektura qurulmazdan öncə təşkilatın real ehtiyacları müəyyən edilməlidir. Bu mərhələ aşağıdakıları əhatə edir:

- təşkilatın biznes məqsədləri və kritik xidmətləri;
- məlumatların növləri və həssaslıq səviyyəsi;
- mövcud infrastrukturun topologiyası və zəif nöqtələri;
- hüquqi və norma tələbləri (məsələn, ISO 27001, GDPR və s.).

Bu təhlil arxitekturanın düzgün prioritetlərlə qurulmasına, resursların optimal bölüşdürülməsinə və müdafiə mexanizmlərinin real risklərə uyğun seçilməsinə imkan verir.[1]

2. Risklərin qiymətləndirilməsi və təhlükə modelləşdirilməsi

Kibertəhlükəsizlik arxitekturasının dayanacağı əsas sütun risk analizi və təhlükə modelləşdirilməsidir. Burada məqsəd:

- mümkün hücum vektorlarını və təhdid aktorlarını (threat actors) müəyyənləşdirmək;
- onların təsir (impact) və ehtimal (likelihood) səviyyəsini qiymətləndirmək;
- risklərə uyğun təhlükəsizlik nəzarətləri (security controls) seçməkdir.[2]

Təhlükə modelləşdirilməsi nəticəsində arxitekturanın hansı qatında hansı müdafiə vasitəsinin vacib olduğu aydınlaşır.

3. "Defense-in-Depth" (dərinlik üzrə müdafiə) yanaşması

Tək bir müdafiə alətinə güvənmək arxitektura baxımından zəiflik yaradır. Buna görə "Defense-in-Depth" yanaşması tətbiq olunur. Bu prinsipə görə təhlükəsizlik bir neçə qatda qurulur:

- Perimetr səviyyəsi (Firewall, WAF, IDS/IPS)
- Şəbəkə səviyyəsi (segmentasiya, NAC, VPN)
- Sistem və server səviyyəsi (hardening, EDR)
- Tətbiq və məlumat səviyyəsi (şifrələmə, IAM, DLP).

Belə çoxqatlı struktur hücumun bir mərhələdə keçməsinə imkan verməsə də, digər qatlarda qarşısını almağa şərait yaradır.

4. Şəbəkə segmentasiyası və Zero Trust modeli

Şəbəkə segmentasiyası təşkilatın daxili mühitində lateral movement (şəbəkə daxilində yayılma) riskini azaldır. Bu məqsədlə:

- şəbəkə zonalara bölünür (DMZ, daxili LAN, server zonası, istifadəçi zonası);
- kritik sistemlər ayrı segmentlərdə saxlanılır;
- girişlər "minimum səlahiyyət" (least privilege) prinsipi ilə idarə olunur.[6]

Bundan əlavə, Zero Trust modeli "heç kimə avtomatik etibar etmə" prinsipinə əsaslanır. Yəni daxili şəbəkədə belə hər sorğu identifikasiya və verifikasiya edilir.

5. İdentifikasiya və girişlərin idarə edilməsi (IAM)

Arxitekturanın ən kritik hissələrindən biri istifadəçi və sistem girişlərinin düzgün idarə olunmasıdır. IAM çərçivəsində:

- MFA (multi-factor authentication) tətbiq olunur;
- rol əsaslı səlahiyyət modeli (RBAC) qurulur;
- servis hesabları və API açarları idarə edilir;
- istifadəçi həyat dövrü (onboarding/offboarding) avtomatlaşdırılır.

IAM düzgün qurulmadıqda istənilən texniki müdafiə zəifləmiş olur.

6. Təhlükəsiz konfiqurasiya və sistem sərtləşdirilməsi (Hardening)

İstənilən sistem standart konfiqurasiya ilə istifadəyə verildikdə çoxlu açıq zəifliklər saxlayır. Hardening prosesi aşağıdakı tədbirləri əhatə edir:

- lazımsız servislərin söndürülməsi;
- defolt parolların dəyişdirilməsi;
- OS və tətbiq səviyyəsində təhlükəsizlik siyasətlərinin tətbiqi;
- patch management (yeniləmə idarəetməsi).

Bu istiqamət arxitekturanın "texniki bünövrəsini" möhkəmləndirir.

7. Davamlı monitorinq və logların mərkəzləşdirilməsi (SIEM/SOC)

Arxitektura təkcə qoruma deyil, həm də aşkarlama və reaksiya qabiliyyətini təmin etməlidir. Bunun üçün:

- loglar mərkəzləşdirilir (SIEM platformasına toplanır);[5]
- anomaliya aşkarlama qaydaları qurulur;
- real vaxt xəbərdarlıq sistemi işləyir;
- SOC (Security Operations Center) prosesləri təyin olunur.

Monitorinq arxitekturanın "gözləri" rolunu oynayır və hücumların erkən mərhələdə tapılmasını təmin edir.

8. Hadisələrə cavab mexanizmi (Incident Response Architecture)

Təhlükəsizlik arxitekturası insident zamanı necə davranacağını əvvəlcədən bilməlidir. IR mexanizmi:

- insident kateqoriyalarını;
- cavab addımlarını (containment, eradication, recovery);
- məsuliyyət bölgüsünü;
- kommunikasiya və eskalasiya qaydalarını müəyyən edir.

Bu plan olmadan ən yaxşı arxitektura belə insidentdə gecikə və ciddi zərər yarada bilər.

9. Backup və Business Continuity inteqrasiyası

Arxitektura yalnız hücumu dayandırmaq yox, organizasiyanın fəaliyyətini bərpa etmək üçün də qurulur. Burada:

- kritik məlumatların müntəzəm backup edilməsi;[3]
- backup-ların offline/immutable saxlanması;
- DR (Disaster Recovery) ssenarilərinin test edilməsi;
- biznes davamlılığı planı ilə inteqrasiya vacibdir.

Xüsusilə ransomware ssenarilərində bu qat "son müdafiə xətti" sayılır.

10. İnsan faktoru və təhlükəsizlik mədəniyyəti

Arxitektura yalnız texnologiyadan ibarət deyil. İnsan səhvləri və sosial mühəndislik hücumları ən böyük risklərdəndir. Buna görə:

- işçilərə mütəmadi təlimlər keçirilməli;
- phishing simulyasiyaları tətbiq olunmalı;
- təhlükəsizlik siyasətləri hamı üçün aydın olmalıdır;
- təşkilatda təhlükəsizlik mədəniyyəti formalaşdırılmalıdır.

Texniki arxitektura insan faktorunu nəzərə almadıqda dayanıqlılıq zəifləyir.

Nəticə. Kibertəhlükəsizlik arxitekturasının qurulması təşkilatın rəqəmsal mühitdə dayanıqlı, idarə olunan və davamlı şəkildə fəaliyyət göstərməsi üçün əsas şərtdir. Arxitektura risk analizindən başlayaraq çoxqatlı müdafiə, şəbəkə segmentasiyası, IAM, hardening, monitorinq, insident cavab planı, backup və insan faktoruna qədər uzanan kompleks bir sistemdir.

Bu komponentlərin bir-biri ilə inteqrasiya olunmuş şəkildə qurulması təşkilata hücumlardan əvvəl qorunmaq, hücum zamanı vaxtında aşkarlamaq və hücumdan sonra sürətli bərpa imkanları yaradır. Nəticə etibarilə düzgün planlaşdırılmış kibertəhlükəsizlik arxitekturası informasiya resurslarının qorunmasını təmin etməklə yanaşı, təşkilatın reputasiyasını, müştəri etibarını və ümumi əməliyyat davamlılığını da gücləndirir.

Ədəbiyyat siyahısı

1. ISO, (2022), ISO/IEC 27001:2022, Information Security Management Systems (ISMS), Requirements, International Organization for Standardization. / [Elektron resurs] / - 16 fevral, 2025. URL: http://www.iso.org/standard/27001
2. NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. / [Elektron resurs] / - 13 fevral, 2025. URL: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology. / [Elektron resurs] / - 16 fevral, 2025. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. CIS. (2021). CIS Critical Security Controls v8 (v8.1). Center for Internet Security. / [Elektron resurs] / - 18 fevral, 2025. URL: http://www.cisecurity.org/controls/v8
5. NIST. (2020). *NIST Special Publication 800-92 — Guide to Computer Security Log Management.* National Institute of Standards and Technology. / [Elektron resurs] / - 16 fevral, 2025.
URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
6. Rose S., Borchert O., Mitchell S., & Connelly S., (2020), Zero Trust Architecture (NIST SP 800-207), National Institute of Standards and Technology / [Elektron resurs] / - 16 fevral, 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

BUILDING A CYBERSECURITY ARCHITECTURE: A SYSTEMATIC AND RESILIENT APPROACH IN ORGANIZATIONS

I.I. Seyfullayev, S.T. Aliyeva
Azerbaijan University, Jeyhun Hajibeyli 71, Baku, Azerbaijan

Abstract: In the modern digital environment, cyber threats are becoming more complex and persistent, making cybersecurity architecture a critical component for organizations. Building a well-structured cybersecurity architecture enables the systematic protection of information assets, ensures business continuity, and enhances resilience against attacks. This study focuses on the development of a layered and sustainable cybersecurity architecture that integrates people, processes, and technology. Key architectural elements such as risk management, network segmentation, access control, security monitoring, and incident response are discussed. By adopting a holistic and proactive approach, organizations can strengthen their defense mechanisms, reduce vulnerabilities, and achieve long-term cybersecurity resilience.

Keywords: Cybersecurity architecture, system security, risk management, resilience, organizational security.