DOI: https://doi.org/10.36719/2789-6919/57/212-216

Namiq Quliyev
Odlar Yurdu Universiteti
magistrant
https://orcid.org/0009-0009-4332-7197
nquliyevcorp@gmail.com

IOT cihazlarının təhlükəsizliyi və kiber-təhlükə riskləri

Xülasə

Tədqiqatın məqsədi: Bu tədqiqatın məqsədi, vacib inkişaf sahələrində və vacib infrastrukturda IoT cihazlarının idarə olunmasına təsir göstərə biləcək vacib idarəetmə problemlərini və risklərini tapmaqdır. Tədqiqatın məqsədi, IoT infrastrukturundakı zəiflikləri, o cümlədən aparat dizayn qüsurlarını, tətbiq proqram təminatındakı çatışmazlıqları, şəbəkə konfiqurasiya səhvlərini və təchizat zənciri təhdidlərini sistematik şəkildə araşdırmaqdır.

Tətbiqi əhəmiyyəti: Tədqiqat nəticələri bizə inkişaf etməkdə olan IoT ekosistemləri üçün vacib olan kibertəhdidlərdən, məsələn, kritik infrastruktur, səhiyyə sistemləri, sənaye əməliyyatları və gündəlik istehlakçı tətbiqlərindən qorunmaq üçün faydalı bir yol təqdim edir. Təşkilati riskləri azaltmaq üçün texniki, təşkilati və strateji müdafiə mexanizmlərinin tətbiqi üçün praqmatik strategiyalar təklif edir.

Tədqiqat nəticəsi: IoT təhlükəsizliyinin yalnız bir və ya iki texnoloji düzəliş deyil, geniş bir strategiyaya ehtiyacı var. Son nöqtə cihazları, şəbəkə seqmentasiyası, bulud API təhlükəsizliyi və məlumatların təmin edilməsi bu strategiyanın vacib hissələridir. Tədqiqat, həmçinin, gələcək risklərlə mübarizə aparmaq üçün real vaxt rejimində şeyləri izləməyin, proqram təminatının monitorinqini yoxlamağın və kvant sonrası kriptoqrafiya standartına keçməyin nə qədər vacib olduğunu vurğulayır.

Açar sözlər: *IoT təhlükəsizliyi, kibertəhlükəsizlik riskləri, şəbəkə seqmentləri, son nöqtə qorunması, bulud API-ləri, məlumatların təmin edilməsi, təchizat zənciri təhlükəsizliyi, kvant sonrası kriptoqrafiya, ağıllı cihazlar, proqram təminatı ilə dəstəklənən, identifikasiya, sıfır zəifliklər*

Namig Guliyev
Odlar Yurdu University
Master's student
https://orcid.org/0009-0009-4332-7197
nquliyevcorp@gmail.com

Security and Cyber Threat Risks of Iot Devices

Abstract

Research objective: The goal of this study is to find important governance problems and risks that could affect the management of IoT devices in important growth areas and important infrastructure. The study's objective is to systematically examine vulnerabilities within IoT infrastructure, encompassing hardware design flaws, application software deficiencies, network configuration mistakes, and supply chain threats.

Practical significance: The research results give us a useful way to protect against cyberthreats that are important to the IoT ecosystems that are developing, like critical infrastructure, healthcare systems, industrial operations, and everyday consumer apps. It proposes pragmatic strategies for the implementation of technical, organizational, and strategic defense mechanisms to alleviate organizational risks.

Research conclusion: IoT security needs a broad strategy, not just one or two technological fixes. Endpoint devices, network segmentation, cloud API security, and data provisioning are all important parts of this strategy. The study also stresses how important it is to monitor things in real time, check software monitoring, and switch to a post-quantum cryptography standard to deal with future risks.

Keywords: *IoT security, cybersecurity risks, network segments, endpoint protections, cloud APIs, data provisioning, supply chain security, post-quantum cryptography, smart devices, software-assisted, authentication, zero vulnerabilities*

Giriş

Müasir dünyada IoT texnologiyaları həyatımızın böyük bir hissəsinə çevrilib. Sensorlar, kameralar, tibbi cihazlar, sənaye nəzarətçiləri, ağıllı sayğaclar və qoşulmuş avtomobillər kimi IoT cihazları gündəlik həyatımız, biznes əməliyyatlarımız və milli müdafiə sistemlərimiz üçün çox vacibdir. Bu cihazlar daha yaxşı ictimai təhlükəsizlik, daha yüksək səmərəlilik və yeni xidmətlər kimi böyük sosial və iqtisadi faydalar vəd edir. Bununla belə, onlar hakerlərin hücum etməsini də asanlaşdırır. Bu vəd ilə təhdid arasındakı ziddiyyət 2025-ci ildə kibertəhlükəsizlik üçün böyük problem olacaq (SecurityScorecard, 2024).

Dünyada getdikcə daha çox IoT cihazı var. 2024-2025-ci illərə qədər 18-19 milyard qoşulmuş IoT cihazının olması gözlənilir və bu rəqəmin 2034-cü ilə qədər 40 milyarddan çox olacağı gözlənilir (SecurityScorecard, 2024). Bütün bu cihazlar səbəbindən inventarlaşdırılmalı, təhlükəsizləşdirilməli, yenilənməli və idarə olunmalı milyardlarla yeni son nöqtə var. Ölçü artımı, həmçinin, kibertəhlükəsizlik risklərinin eksponensial sürətlə artmasına səbəb olur.

Tədqiqat

2024-cü ilin məlumatlarına görə (Alnaim, 2023), hər üç kiberhücumdan birinin artıq IoT cihazlarından istifadə edəcəyi gözlənilir. 2025-ci ilin sonuna qədər kibercinayətkarlığın ildə 10,5 trilyon dollara başa gələcəyi gözlənilir ki, bu da IoT cihazlarının kiberhücumlarda nə qədər vacib olduğunu göstərir (Alnaim, 2023).

Şəkil 1. 2025-ci il üçün əsas IoT haker statistikası və təhdid mənzərəsi.

Bu məqalədə Əhəmiyyətli IoT cihazlarının təhlükəsizlik baxımından üzləşdiyi problemlər, kibertəhlükəsizliklə bağlı risklər və bu risklərin qarşısını almaq üçün atılan addımlar haqqında danışılır. Məqsəd, IoT ekosistemində təhlükəsizliyin təmin edilməsi üçün texniki, təşkilati və siyasi yanaşmaların əhəmiyyətini vurğulamaqdır.

Əsas risklər və boşluqlar. İndi çox sayda insan Əhəmiyyətli IoT cihazlarından istifadə etdiyi üçün ciddi təhlükəsizlik problemləri mövcuddur. Əhəmiyyətli IoT ekosisteminin unikal xüsusiyyətlərinə görə ənənəvi kibertəhlükəsizlik metodları kifayət etməyə bilər. Əsas risk dəyişənləri və boşluqlar aşağıdakılardır:

Dizaynla gələn təhlükəsizlik problemləri (Insecurity-by-Design). Bir çox IoT cihazı istehsalçısı, məhsulların bazara çıxarılma müddətini qısaltmaq və xərcləri azaltmaq məqsədilə təhlükəsizlikdən çox funksionallığa üstünlük verir. Bu yanaşma, cihazların "dizaynla gələn təhlükəsizliksizlik" (insecurity-by-design) problemi ilə üzləşməsinə səbəb olur. Nəticədə, cihazlar standart parollar, şifrələnməmiş telemetriya, sərt kodlanmış açarlar və uzaqdan proqram təminatını yeniləmək üçün məhdud imkanlar kimi zəifliklərlə buraxılır. Forescout-un 2025-ci il hesabatı, İT, IoT, OT və tibbi

IoT cihazlarında zəifliklərin artdığını göstərir ki, bu da müəssisələr və kritik infrastruktur üçün qəbuledilməz risklər yaradır (Prince et al., 2024).

Zəif giriş nəzarəti və identifikasiya. Bir çox IoT cihazının zəif və ya standart parolları var ki, bu da böyük problemdir. Araşdırmalara görə, cihazların təxminən 20%-i hələ də yeni olduqları zaman gələn parollardan istifadə edir. Bu, hücum edənlərin cihazlara daxil olmasını və "LapDogs" kampaniyası (Maned et al., 2026) kimi botnetlərə qoşulmasını asanlaşdırır. Çoxfaktorlu identifikasiya (MFA) kimi güclü identifikasiya metodlarının olmaması kiminsə icazəsiz daxil olma ehtimalını artırır.

Köhnə proqram təminatı və yeniləmədə çətinlik. IoT cihazları uzun müddət işləyir, lakin istehsalçılar onları yalnız qısa müddət dəstəkləyir. Bu o deməkdir ki, proqram təminatı və təhlükəsizlik boşluqları açıq qalır. Bir çox cihazın uzaqdan yenilənmə qabiliyyəti olmadığı və ya çox mürəkkəb olduğu üçün zəifliklərı tez bir zamanda düzəltmək çətindir. Bu, cihazları "sıfır günlük" hücumlara və məlum zəifliklərin istifadəsinə açıq edir (IEEE Xplore, 2021).

Şəbəkəni seqmentlərə bölməmək və səhv qurmaq. Şirkətlər və fabriklər tez-tez IoT cihazlarını şəbəkələrinə qoşurlar. Lakin bu cihazlarda kifayət qədər şəbəkə seqmentasiyası (mikro-seqmentasiya kimi) yoxdursa, təcavüzkarlar şəbəkə boyunca yan tərəfə keçə və IoT cihazı haker hücumuna məruz qaldıqda daha vacib sistemlərə keçə bilərlər. Təhlükəsizlik boşluqları düzgün qurulmamış şəbəkə parametrlərindən də yaranır.

Təchizat zəncirindəki risklər. IoT cihazlarını yaratmaq mürəkkəb bir təchizat zənciri tələb edir. Üçüncü tərəf hissələri, proqram təminatı kitabxanaları və xidmətləri görmək çətin ola bilər ki, bu da təchizat zəncirindəki zəif cəhətləri gizlədə bilər. Təchizat zəncirindəki hər hansı bir zəiflik son məhsulu daha az təhlükəsiz edə bilər (Arif və b., 2025). Proqram Təminatı Materialları Qanunu (SBOM) kimi standartlara əməl edilməməsi bu riski daha da artırır.

Məlumatların məxfiliyi və təhlükəsizliyi. IoT cihazları getdikcə daha həssas məlumatlar toplayır və göndərir. Şifrələmənin olmaması məlumatlara daxil ola və ya onları dəyişdirə bilməyən insanların bunu etməsini mümkün edir. Məlumat göndərərkən zəif şifrələmə alqoritmlərindən istifadə etmək və ya şifrələmə protokollarını (məsələn, TLS/SSL) səhv tətbiq etmək həmin məlumatların məxfiliyini və təhlükəsizliyini risk altına qoyur (MDPI Sensors, 2021).

Kvant hesablamasının riskləri (Kvantdan sonrakı risk). Kvant hesablamaları gələcəkdə mövcud şifrələmə standartlarını daha az təhlükəsiz edə bilər. TechRadar bildirir ki, 2035-ci ilə qədər dünyada 1 milyarddan çox ağıllı sayğac kvant hücumlarından qorunmaq üçün PQC (Kvantdan Sonrakı Kriptoqrafiya) standartlarına yenilənməlidir (Jurcut et al., 2020). Bir çox köhnə IoT cihazlarının dəyişdirilməsi yeganə seçim ola bilər, çünki onlar uzaqdan proqram təminatı yeniləmələrini ala bilmirlər. Bu, baha başa gələ bilər.

Bu risklər, IoT ekosisteminin mürəkkəbliyi və müxtəlifliyi ilə birlikdə, kibertəhlükəsizlik mütəxəssislərinin işlərini görməsini çox çətinləşdirir. Növbəti hissədə bu riskləri azaltmağın yolları və bunu etməyin ən yaxşı yolları haqqında danışılacaqdır.

Həllər və ən yaxşı təcrübələr. Başlanğıcda, IoT cihazlarının təhlükəsizliyini təmin etmək eyni zamanda bir çox fərqli metoddan istifadə etmək deməkdir. Şirkət qaydaları və hökumət siyasətləri texnoloji düzəlişlər qədər vacibdir. Güclü parollar və müntəzəm yeniləmələr riskinizi azaltmaq üçün edə biləcəyiniz ən yaxşı iki şeydir. Başqa bir seçim, ağıllı cihazlar üçün ayrı şəbəkələr qurmaqdır ki, bir şey səhv getsə, giriş məhdudlaşdırılsın. İstifadəçi təlimi bəzən nəzərdən qaçırılır; insanların təhlükəsiz qalmaları üçün aydın təlimatlara ehtiyacı var. İşlərə nəzarət edən müstəqil qruplar onları daha etibarlı edə bilər. Nəhayət, istehsalçılar satın alındıqdan sonra dəyişdirilə bilən məhsullar hazırlamalıdırlar.

IoT son nöqtələri üçün qorunma. IoT cihazlarını daha təhlükəsiz etməyin bir yolu, təhlükəsizliyi birbaşa cihazda daha güclü etməkdir. Şirkətlər TCP və UDP portları kimi haker hücumuna daha çox məruz qalma ehtimalı olan rabitə kanallarına diqqət yetirərək pozuntu risklərini azalda bilərlər. Problem yaranmazdan əvvəl, təhlükəsiz olmayan məlumat ötürülməsi dayandırılır. Kimsə kompüterinizə zərərli proqram təminatı yerləşdirməyə çalışdıqda, müdafiəniz işə düşür. Bu təbəqəni qoruyan şirkətlər müasir ransomware variantları kimi yeni təhdidlərlə daha yaxşı mübarizə apara

bilirlər. Təhlükəsizlik qrupları hər bir qoşulmuş maşını aydın görə bilirlər. Real vaxt rejimində yeniləmələr cihazların infrastruktur boyunca necə işlədiyini göstərir. Nəzarət daha sərt olduqda zəif nöqtələr daha kiçik olur (MDPI Sensors, 2022).

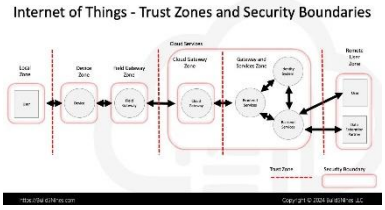
Şəkil 2 göstərir ki, son nöqtə təhlükəsizliyi bir neçə təbəqədə baş verir.

Aşkarlama qarşısının alınmasından aşağıdır və hər birinin işləməsinə kömək etmək üçün öz alətlər dəsti var. Cavab təhdidlər əvvəlki addımları atladıqdan sonra gəlir. Təbəqələr tək bir nəzarət nöqtəsinə ehtiyac olmadan birlikdə işləyir. Qoruma zamanla artır və təhdidlər dəyişdikcə dəyişir.

IoT Şlüzləri üçün təhlükəsizlik. Təhdidlər daha mürəkkəbləşdikcə, müəssisələr qoşulmuş cihazlarını qorumaq üçün IoT şlüz təhlükəsizliyindən istifadə edirlər. Bu tip sistemlər cihazların internetə necə daxil olduğunu idarə edir və viruslar kimi zərərli proqramların şəbəkə yollarını ələ keçirməsinin qarşısını alır (Morgan, 2020). Təhlükəsiz Veb Şlüz və digər alətlər tətbiqləri idarə etmək, şifrələnmiş veb trafikini skan etmək, uzaqdan baxış sessiyalarını təcrid etmək və veb sayt ünvanlarını yoxlamaq kimi vacib xüsusiyyətlər təklif edir. Müəssisələr bulud platformalarına və ofis xaricindən girişə daha çox güvəndikcə bu təbəqələr getdikcə daha vacib hala gəlir. Onlar ağıllı cihazları xaricdən və ya korporativ şəbəkələrin daxilindən gələn hücumlardan qoruyur və onlayn mübadilə ilə bağlı riskləri azaldır (Schiller et al., 2022).

Bulud API-ləri üçün təhlükəsizlik. IoT cihazları bulud əsaslı API-lər vasitəsilə bir-birinə qoşulduqda, məlumatları asanlıqla paylaşa bilərlər. Bu bağlantılar əməliyyatlar üçün çox vacib olduğundan, tək bir zəif nöqtə çoxlu məlumatın sızmasına səbəb ola bilər. Bu riskləri azaltmaq üçün doğrulama addımları, şifrələnmiş köçürmələr, rəqəmsal açarlar və trafik nəzarətçiləri kimi təhlükəsizlik tədbirlərindən istifadə olunur. Veb API təhlükəsizlik tədbirləri məlumatları şəbəkələr arasında hərəkət edərkən qoruyur. REST tipli interfeyslər, həmçinin, aparat və mərkəzi bölmələr arasında göndərilən məlumatları qorumaq üçün qarışıq üsullardan istifadə edir. Bu giriş nöqtələrinin nə qədər yaxşı idarə olunması, əlaqəli mühitlərin nə qədər sabit olduğunu tez-tez müəyyən edir.

Ayrı-ayrı hissələrlə təhlükəsiz şəbəkə qurmaq. Şəbəkədə düzgün giriş nəzarətinin qurulması təhlükəsizliyin ilk addımıdır. Bu qaydalar tətbiq edildikdən sonra yalnız etibarlı və təsdiqlənmiş avadanlıqlar daxil ola bilər (Fortinet, 2023). Müdafiənin ilk addımı güclü bir firewall-a sahib olmaqdır. Bundan sonra, istifadəçilər daxil olmağa çalışdıqda cihazları qoruyan çoxfaktorlu identifikasiya (MFA) kimi şeylər vasitəsilə müdafiə güclənir. Doğrulama açarlarının qorunması təhlükəsizliyin ilk addımıdır və yeni antivirus vasitələri təhdidlərin yayılmasından əvvəl qarşısını almağa kömək edə bilər (Schiller et al., 2022). Bir cihaz sıradan çıxdıqda, seqmentləşdirilmiş şəbəkələr pozuntuları erkən dayandıraraq zərəri məhdudlaşdırır. Trafik izləmək qəribə davranışlar göstərə bilər ki, bu da tez-tez bir şeyin səhv olduğunun ilk əlamətidir. İzolyasiya təcavüzkarları yavaşlatır ki, bu da sistemlərə özləri cavab vermək üçün vaxt verir.



Şəkil 3, etibar zonalarını və onların qoruyucu sərhədlərini göstərməklə IoT təhlükəsizliyinin necə işlədiyini göstərir.

Məlumatların qorunması və şifrələnməsi. Çox vaxt nəzərə alınmasa da, fayllar bağlantılar arasında, xüsusən də onlayn və ya cihazlar arasında hərəkət edərkən məlumatların qarışdırılması çox vacibdir. Ağıllı cihazlara gəldikdə, məlumatların kilidlənməsi adətən həm paylaşılan açarlı, həm də ikili açarlı sistemlərdən istifadə etmək deməkdir. Bir metod məzmunu gizlətmək və göstərmək üçün eyni kodlardan istifadə edir, digəri isə daha güclü qoruma təmin etmək üçün qoşalaşmış, lakin fərqli açarlardan - biri açıq, digəri isə gizli - istifadə edir (Anedda et al., 2023). Rəqəmsal seyflərdə və ya fiziki disklərdə saxlanılan həssas məlumatları qorumaq üçün etibarlı təhdid aşkarlama proqramına, müasir virus qorunmasına və IoT risklərini erkən aşkar etmək üçün trafiki canlı izləyən vasitələrə ehtiyacınız var.

Nəticə

Təchizat zəncirinin yoxlanılması və firmware mənşəyi. Şirkətlər komponentlərin haradan gəldiyini sübut edən sübutlar, təsdiqlənmiş proqram təminatı mənbələri və ətraflı proqram təminatı inventarları tələb etdikdə, təchizat zəncirləri daha aydın olur. Onlar həmçinin qüsurları bildirmək üçün eyni metodlardan istifadə etməlidirlər. Çoxlu sayda problemi olan sistemlər üçün müqavilələr formatların istifadəsini tələb etməlidir. Təchizatçılar daha aydın görə bildikdən sonra problemləri erkən mərhələdə tapmaq və həll etmək daha asan olur.

Ədəbiyyat

1. Arif, H., Ali, A. K. S., & Nabi, H. A. (2025). IoT Security through ML/DL: Software Engineering Challenges and Directions. *ICCK Journal of Software Engineering*.
2. Anedda, M., Floris, A., Girau, R., Fadda, M., & Ruiu, P. (2023). *Privacy and Security Best Practices for IoT Solutions*. IEEE Access.
3. Alnaim, A.K. (2023). *Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security*.
4. Fortinet. (2023). *IoT Security Best Practices? How To Protect IoT Devices*. https://www.fortinet.com/resources/cyberglossary/iot-best-practices
5. IEEE Xplore. (2021). *A survey on emerging SDN and NFV security mechanisms for IoT systems*.
6. Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). *Introduction to IoT security, IoT security: advances in*.
7. Maned, V. R., Rath, S., & et al. (2026). *Enhancing IoT security through cloud-assisted post-quantum authentication: a case study with UOV signatures*. Scientific Reports.
8. Morgan, S. (2020). *Cybercrime to Cost The World $10.5 Trillion Annually By 2025*.
9. MDPI Sensors. (2021). *Semantic-Eware Security Orchestration in SDN/NFV-Enabled IoT Systems*.
10. MDPI Sensors. (2022). *Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions*.
11. Prince, N. U., Al Mamun, M. A., Olajide, A. O., & Sani, A. (2024). IEEE Standards and Deep Learning Techniques for Securing Internet of Things (IoT) Devices Against Cyber Attacks. *Journal of Computer Science and Technology*.
12. *Security Scorecard*. (2024). LapDogs. The New ORB in Town.
13. Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., & Ziörjen, M. (2022). *Landscape of IoT security, Computer Science*.

Daxil oldu: 08.01.2026
Qəbul edildi: 10.04.2026