PARADIGMA, No.2, 2025, səh.180-185
https://doi.org/10.30546/30015.2025.2.153

KİBER HÜCUMLAR VƏ ONLARIN QARŞISININ ALINMASI ÜSULLARI

N.D. Cəfərov, D.M. İsgəndərzadə
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: dunyamaly.isgandarzada@student.au.edu.az

Xülasə. Rəqəmsal dövrdə kiberhücumlar texnoloji olmaqla yanaşı, sosial-təşkilati problemlər də yaradır. Bu təhdidlərlə mübarizədə texnoloji və insani amilləri birləşdirən balanslaşdırılmış yanaşma vacibdir. Təhlükəsizlik təkcə texniki vasitələrlə deyil, istifadəçi məlumatlılığı və kibertəhlükəsizlik mədəniyyəti ilə də təmin olunur. Kiber davamlılığı artırmaq üçün qabaqlayıcı tədbirlər, davamlı investisiyalar, gücləndirilmiş qanunvericilik və strukturlaşdırılmış təlim proqramları zəruridir. Nəticə olaraq, kibertəhlükəsizlik strateji prioritetdir və gələcək rəqəmsal mühitin təhlükəsizliyi bugünkü addımlardan asılıdır.

Açar sözlər: Kiber hücum, kibertəhlükəsizlik, texnologiya, İKT, təhlükəsizlik

Giriş

Müasir dünyada informasiya texnologiyalarının sürətlə inkişaf etməsi həyatımızın bütün sahələrinə təsir göstərir. Bu inkişaf bir tərəfdən informasiya axınının və rəqəmsal xidmətlərin genişlənməsinə şərait yaradırsa, digər tərəfdən yeni təhlükələr və risklərlə də müşayiət olunur. Xüsusilə kiber məkanın genişlənməsi, fərdi və təşkilati məlumatların internet üzərindən idarə olunması, bu sahədə təhlükəsizliyin təmin olunmasını vacib edir [5]. Kiber hücumlar bu təhlükələrin əsas mənbəyidir və həm fərdi istifadəçilər, həm də təşkilatlar üçün ciddi problemlər yarada bilir.

Kiber hücum – kompüter sistemlərinə, şəbəkələrə, proqram təminatına və məlumat bazalarına qanunsuz müdaxilə cəhdidir. Bu müdaxilələr adətən informasiya oğurluğu, xidmətlərin dayandırılması, sistemin idarəsinin ələ keçirilməsi və ya məlumatların pozulması məqsədi ilə həyata keçirilir. Hücumlar fərqli formalar ala bilər və onların arxasında bəzən fərdi hakerlər, bəzən də təşkilatlanmış kiber cinayətkar qruplar və ya hətta dövlət dəstəyi ilə fəaliyyət göstərən strukturlar dayanır [3]. Kiber hücumların təsiri, pozduğu sistemin həssaslığına və hücumun məqsədinə görə dəyişə bilər – şəxsi məlumatların sızmasından tutmuş, iri maliyyə itkilərinə və milli təhlükəsizlik problemlərinə qədər geniş bir spektri əhatə edə bilər.

Rəqəmsallaşmanın artması ilə birlikdə kiber təhlükələr də daha mürəkkəb və tez-tez rast gəlinən hala gəlmişdir. Onlayn bankçılıq, elektron hökumət xidmətləri, bulud texnologiyaları, ağıllı cihazlar və sosial media platformaları istifadəçilərin gündəlik həyatının ayrılmaz hissəsinə çevrilmişdir [3]. Bu texnologiyalar istifadəçilərə rahatlıq gətirsə də, onların arxasında zəif təhlükəsizlik tədbirləri olduqda böyük risklər doğurur. Hakerlər bu zəif nöqtələrdən istifadə edərək fərdi məlumatları oğurlayır, sistemləri sıradan çıxarır və maliyyə vəsaitlərini ələ

keçirirlər. Son illərdə dünyada geniş rezonans doğuran “ransomware” (şifrə qoyub pul tələb edən viruslar), “phishing” (aldadıcı e-poçt və mesajlar) və “DDoS” (xidmətin göstərilməsinə mane olan hücumlar) kimi kiber hücum növlərinin yayılması bu təhlükənin real və geniş miqyaslı olduğunu bir daha sübut edir.

Bu araşdırmanın əsas məqsədi rəqəmsal dövrdə geniş yayılmış kiber hücum növlərini sistemli şəkildə təhlil etmək və onlara qarşı effektiv müdafiə üsullarını təqdim etməkdir. Məqalədə həm texniki, həm də təşkilati səviyyədə tətbiq oluna bilən mühafizə strategiyaları göstəriləcək. Hər bir kiber hücum növü üçün real nümunələr və bu hücumlara qarşı istifadə edilən texnologiyalar – şifrləmə, firewall sistemləri, antivirus proqramları, təlimatlar və istifadəçi maarifləndirilməsi kimi tədbirlər təqdim olunacaq. Məqsəd yalnız problemi təqdim etmək deyil, eyni zamanda oxuculara praktiki baxımdan faydalı və tətbiq oluna bilən həll yolları təqdim etməkdir.

Kiber hücumların müxtəlif növləri mövcuddur və onların hər biri özünəməxsus metodlarla həyata keçirilir. Aşağıda ən geniş yayılmış və təhlükəli hesab edilən kiber hücum növləri izah olunur:

1. Fişinq (Phishing)

Fişinq hücumları – istifadəçiləri aldadaraq onların şəxsi məlumatlarını (parollar, bank məlumatları, şəxsiyyət məlumatları və s.) ələ keçirməyə yönəlmiş saxtakarlıq üsuludur. Bu hücumlar adətən e-mail, SMS və ya saxta veb səhifələr vasitəsilə həyata keçirilir [1]. Hücum edən şəxs özünü bank əməkdaşı, dövlət qurumu və ya etibarlı bir təşkilat kimi təqdim edərək istifadəçini saxta linkə daxil olmağa və ya şəxsi məlumatları paylaşmağa vadar edir.

2. Zərərli Proqramlar (Malware, Virus, Trojan)

Zərərli proqramlar kompüter sistemlərinə gizli şəkildə daxil olaraq onların fəaliyyətinə zərər vurmaq və ya məlumatları oğurlamaq üçün hazırlanır. Bu proqramlara viruslar, trojanlar, spyware (gizli izləmə proqramları) və digər növlər daxildir. Onlar çox zaman istifadəçinin xəbəri olmadan e-maillərə əlavə olunmuş fayllar, infeksiyalı proqram yükləmələri və ya şübhəli vebsaytlar vasitəsilə yayılır.

3. DDoS Hücumları (Distributed Denial of Service)

DDoS hücumları – bir və ya bir neçə serverin xidmətini sıradan çıxarmaq üçün həmin sistemə eyni anda çoxsaylı sorğular göndərilməsi ilə həyata keçirilir. Nəticədə sistemlər həddindən artıq yüklənir və fəaliyyətini dayandırır [5]. Bu hücumlar çox zaman siyasi, iqtisadi və ya rəqabət əsaslı motivlərlə edilir və ciddi maddi zərər verəbilir.

4. Ransomware Hücumları

Ransomware hücumları – kompüter sistemindəki məlumatların şifrələnməsi və onların açılması üçün istifadəçidən pul (adətən kriptovalyuta) tələb olunması ilə xarakterizə olunur [5]. Bu hücumlar nəticəsində təşkilatlar və şəxslər öz məlumatlarına çıxışı itirir və bərpa üçün ciddi maliyyə vəsaiti ödəməli olurlar. Ransomware hücumları son illər dünya üzrə ən geniş yayılan kibercinayətlərdən biridir.

5. Man-in-the-Middle Hücumları (MITM)

Bu hücum növü zamanı iki tərəf arasında ötürülən məlumatlarara daxil olmuş üçüncü bir şəxs tərəfindən ələ keçirilir. MITM hücumları xüsusilə ictimai Wi-Fi şəbəkələrində, şifrələnməmiş əlaqələrdə və zəif təhlükəsizlik tədbirləri olan sistemlərdə baş verir. Hücum edən şəxsi stifadəçilərin login məlumatlarını, şəxsi yazışmalarını və digər məxfi məlumatları oğurlayabilər.

6. Brute Force və SQL Injection Hücumları

Brute Force hücumlarında system parolları müxtəlif kombinasiya cəhdləri ilə sındırılmağa çalışılır. Bu metod avtomatlaşdırılmış proqramlar vasitəsilə parol ehtimallarını təkrarlayaraq doğru kombinasiya tapmağa əsaslanır.

SQL Injection isə vebsaytlarda olan zəifliklərdən istifadə edərək verilənlər bazasına zərərli SQL sorğuları daxil etmək yoludur. Bu hücum nəticəsində hücum edən şəxs verilənlər bazasında olan məlumatları oxuya, dəyişdirə və ya silə bilər.

Kiberhücumların sürətlə artdığı müasir dövrdə effektiv müdafiə tədbirləri həyata keçirmək vacibdir. Hücumlara qarşı müdafiə yalnız texnoloji vasitələrlə deyil, həmdə istifadəçi davranışı, maarifləndirmə və təşkilati siyasətlərlə birgə qurulmalıdır. Aşağıda kiber hücumlardan qorunmaq üçün əsas üsullar təqdim olunur:

1. Texniki Təhlükəsizlik Vasitələri

Kibertəhlükələrin qarşısını almağın ilk mərhələsi güclü texniki infrastrukturun qurulmasıdır:

- Antivirus və antispyware proqramları: Kompüterə daxil olan zərərli proqramları aşkar edərək onların sistemə təsiretməsinin qarşısını alır.
- Firewall (od divarı): İcazəsiz giriş cəhdlərini filtrləyir və şübhəli şəbəkə trafikinə nəzarət edir.
- IDS/IPS sistemləri (Intrusion Detection/Prevention Systems): Şəbəkədə baş verən təhdidlərə real vaxt rejimində nəzarət edir və potensial hücumların qarşısını alır.

2. İstifadəçi Səviyyəsində Təhlükəsizlik

İstifadəçilərin şəxsi təhlükəsizlik vərdişləri systemin ümumi müdafiəsinə ciddi təsir edir:

- Güclü və unikal şifrələr: Rəqəm, simvol və böyük-kiçik hərflərdən ibarət kompleks şifrələr istifadə edilməlidir.
- İki faktorlu identifikasiya (2FA): Sistemə giriş zamanı əlavə təhlükəsizlik səviyyəsi təminedir (məsələn, SMS və ya tətbiq vasitəsilə kod).
- Şübhəli linklərdən uzaq durmaq:Tanımadığı şəxslərdən gələn e-maillərdə kilinklərə və ya əlavələrə daxil olmaq təhlükəlidir.

3. Maarifləndirmə və Təlimlər

Kibertəhlükəsizliyin ən zəif halqası istifadəçidir. Bu səbəbdən istifadəçilərin mütəmadi maarifləndirilməsi mühümdür:

- İşçilərin təlimi:Fişinq, zərərli proqramlar və social mühəndislik kimi təhdidlər haqqında təlimlər təşkil olunmalıdır.
- Təhlükəxəbərdarlıqları:İstifadəçilərə dövri olaraq yeni təhdidlər və onların qarşısını alma yolları barədə məlumat verilməlidir.

4. Məlumatların Ehtiyat Nüsxəsi (Backup)

Məlumat itkisi və ya şifrələmə hücumları zamanı bərpa imkanlarının olması həyati əhəmiyyət daşıyır:

- Daimi backup prosesi: Mühüm məlumatlar mütəmadi olaraq yedəklənməli, həm lokal, həmdə bulud sistemlərində saxlanılmalıdır.
- Bərpa testləri: Ehtiyat nüsxələrin işləkliyi mütəmadi olaraq yoxlanılmalıdır.

5. Şifrələməvə VPN İstifadəsi

Məlumatların ötürülməsi zamanı məlumatların gizliliyivə bütövlüyü təmin olunmalıdır:

- Şifrələmə:Məlumatların oxuna bilməsi üçün yalnız səlahiyyətli şəxslərə açar verilir. Bu, məlumat oğurlansa belə, onun istifadəsinin qarşısını alır [4].
- VPN (Virtual Private Network): İctimai və ya təhlükəli şəbəkələrdə təhlükəsiz əlaqə yaratmaq üçün istifadə edilir. Məlumat trafiki şifrələnmiş kanalla ötürülür.

Nəticə

Rəqəmsallaşmanın sürətlə artdığı müasir dövrdə kiberhücumlar təkcə texniki məsələ deyil, həmdə social və təşkilati çağırışdır. Bu hücumların qarşısını effektiv şəkildə almaq üçün həm texnoloji alətlərdən, həmdə insan faktorundan düzgün və balanslı şəkildə istifadə olunmalıdır.

Təhlükəsizlik yalnız antivirus proqramları və şəbəkə sistemləri ilə təmin olunmur – istifadəçilərin maarifləndirilməsi, düzgün şifrə siyasətləri və təhlükəsizlik mədəniyyətinin

formalaşdırılması da mühüm rol oynayır. Kiber risklərə qarşı dayanıqlı systemin qurulması üçün aşağıdakı tövsiyələrə əməl olunması vacibdir:

- Təşkilatlar və fərdi şəxslər kibertəhlükələrə qarşı daha məsuliyyətli olmalı, öz məlumatlarını və cihazlarını qorumaq üçün profilaktik tədbirlər görməlidirlər.
- Kibertəhlükəsizlik sahəsinə daimi investisiya edilməli, yeni texnologiyalar və müdafiə mexanizmləri tətbiq olunmalıdır.
- Dövlət səviyyəsində normativ-hüquqi bazanın gücləndirilməsi və fərdi məlumatların qorunması ilə bağlı qanunların tətbiqi vacibdir.
- Maarifləndirmə və təlimlərin sistemli şəkildə təşkili, xüsusilə dövlət qurumları və korporasiyalar üçün vacibdir.

Sonda qeyd etmək lazımdırki, kibertəhlükəsizlik təkcə texniki məsələ deyil, həmdə strateji prioritetdir. Gələcəyin təhlükəsiz rəqəmsal mühiti, bugunkü tədbirlər və yanaşmalar üzərində qurulacaqdır.

Ədəbiyyat siyahısı

1. Stallings, W. (2016). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education. ISBN: 978-0134527338.
2. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning. ISBN: 978-1337102063.
3. EC-Council. (2021). Certified Ethical Hacker (CEH) v11: Study Guide. Sybex. ISBN: 978-1119800286.
4. National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF) Version 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
5. International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information Security Management Systems. https://www.iso.org/standard/27001.html
6. International Organization for Standardization. (2022). ISO/IEC 27002:2022 - Information Security Controls. https://www.iso.org/standard/75652.html
7. OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. https://owasp.org/Top10/

8. European Union Agency for Cybersecurity (ENISA). (2024). 2024 Report on the State of the Cybersecurity in the Union. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

CYBER ATTACKS AND METHODS OF PREVENTING THEM

D.M.Isgandarzade, N.D.Cafarov
Azerbaijan University, Jeyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. In the digital era, cyberattacks pose not only technological challenges but also socio-organizational issues. Addressing these threats effectively necessitates a balanced approach integrating both technological and human factors. Security is not solely ensured through technical means; user awareness and a robust cybersecurity culture are equally paramount. Enhancing cyber resilience requires proactive measures, sustained investments, a strengthened legislative framework for data protection, and structured training programs. Consequently, cybersecurity constitutes a strategic priority, and the security of the future digital environment hinges upon present actions and approaches.

Keywords: Cyber attack, cybersecurity, technology, IT, security