DOI: https://doi.org/10.36719/2663-4619/101/299-303

Mahmud Məmmədli
Azərbaycan Texniki Universiteti
magistrant
mammadlim98@gmail.com
https://orcid.org/0009-0005-8745-8704
Elvin Abdurəhmanov
Azərbaycan Texniki Universiteti
magistrant
abdurahmanovellvin@gmail.com
https://orcid.org/0009-0000-2259-467X
Aydan Əhədova
Azərbaycan Texniki Universiteti
magistrant
ahadovaaydan@mail.ru
https://orcid.org/0009-0002-9463-9114

KİBER HÜCUMLARINA QARŞI MÜDAFİƏ VƏ FƏALLAŞDIRMA STRATEGİYALARI

Xülasə

Müasir rəqəmsal dövrdə kiberhücumlar daha çox yayılmış və təhlükəli hala gəldi. Bu hücumlar fərdlərin, təşkilatların və hətta dövlətlərin təhlükəsizliyini təhlükə altına alaraq əhəmiyyətli maliyyə və nüfuz itkisinə səbəb ola bilər. Buna görə kiberhücumlardan qorunmaq və təsirlərini azaltmaq üçün təsirli strategiyaların hazırlanması çox vacibdir. Bu araşdırmanın məqsədi kiberhücumlara qarşı təsirli müdafiə strategiyalarını araşdırmaq və hücumları azaltmaq üçün yeni yollar tapmaqdır. Bu strategiyaların əsas məqsədləri informasiya sistemlərinin və rəqəmsal aktivlərin qorunması, hücumların təsirinin minimuma endirilməsi və sürətli bərpanın təmin edilməsidir.

Onilliklər ərzində kibertəhlükəsizlik sahəsində çoxsaylı qiymətləndirmə metodları təklif edilmişdir. Bununla birlikdə, bu məqalədə təsvir olunan ədəbiyyatın sistematik axtarışı onların nəzərdən keçirilməsinin praktik olaraq olmadığını göstərir. Beləliklə, bu tədqiqatın əsas məqsədi elmi ədəbiyyatda təsvir olunan kibertəhlükəsizliyin qiymətləndirilməsi metodlarını hərtərəfli müəyyənləşdirmək və təhlil etməklə bu boşluğu aradan qaldırmaqdır.

Açar sözlər: *Kiberhücum, Zərərli proqram (Malware), Ransomware hücumları, Şəbəkə hücumları, Xidmətdən imtina (DoS) hücumları*

Mahmud Mammadli
Azərbaycan Technical University
master student
mammadlim98@gmail.com
https://orcid.org/0009-0005-8745-8704
Elvin Abdurahmanov
Azərbaycan Technical University
master student
abdurahmanovellvin@gmail.com
https://orcid.org/0009-0000-2259-467X
Aydan Ahadova
Azərbaycan Technical University
master student
ahadovaaydan@mail.ru
https://orcid.org/0009-0002-9463-9114

Defense and activation strategies against cyber attacks

Abstract

In today's digital age, cyber attacks have become more common and dangerous. These attacks can threaten the security of individuals, organizations, and even nations, causing significant financial and reputational losses. Therefore, it is very important to develop effective strategies to protect against and mitigate the effects of cyber attacks.

The purpose of this research is to explore effective defense strategies against cyber attacks and find new ways to mitigate attacks. The main goals of these strategies are to protect information systems and digital assets, minimize the impact of attacks and ensure rapid recovery. Over the decades, numerous assessment methods have been proposed in the field of cybersecurity. However, a systematic search of the literature described in this article shows that their review is practically non-existent. Thus, the main goal of this study is to address this gap by comprehensively identifying and analyzing cybersecurity assessment methods described in the scientific literature.

Keywords: *Cyber attack, Malware, Ransomware Attacks, Network Attacks, Denial of Service (DoS) Attacks*

Giriş

“Kibertəhlükəsizlik” termini ağlımıza gələndə onun müasir texnologiyanın bütün istiqamətlərini əhatə etdiyini düşünməyə meyl edirik. Bu başa düşüləndir, çünki texniki cəhətdən dəqiqdir. Rəqəmsal təhlükəsizlik alətləri inanılmaz dərəcədə çevik hala gəldi - çoxsaylı dizaynların çoxsaylı sənayelərin tərəfindən qəbul edildi.Naviqasiya proqramları, oyun proqramları və sosial media daxil olmaqla əksər cihazlar həmişə internetə qoşulu olur. Eynilə, masaüstü kompüterlər də. İstər mağazaya baxırsınız, istərsə də musiqi dinləyirsiniz - çox güman ki, kibertəhlükəsizliyin müasir tərifləri tələb edən bu əhatəli mühitdə iştirak edirsiniz.Kibertəhlükəsizlik işləri, bu gün rəqəmsal cihazlar arasında göndərilən və alınan məlumatların rəqəmsal müdafiəsini idarə edir, mahiyyət etibarilə şəbəkənin və informasiyanın müdafiəsini təşkil edir. Bu, məlumatların saxlanması, qorunması, hücumların müəyyən edilməsi kiberhücumlara qarşı reaksiyanı ölçür və ən pis vəziyyətlərdə oğurlanmış qiymətli məlumatları, çox vaxt da şəxsi məlumatların bərpasını əhatə edir. Aydındır ki, kibertəhlükəsizliyin əhatə dairəsi olduqca böyükdür (Özdemir, 2023: 88-95).

Bu məqalənin əsas məqsədi, kiber hücumlara qarşı effektiv müdafiə strategiyalarının və fəallaşdırma tədbirlərinin təyin edilməsi və inkişaf etdirilməsidir. Məqsəd, kiber təhlükəsizlik prinsiplərinin və tədbirlərinin araşdırılması bu sahədəki çoxsaylı təhlükələrə qarşı cəmiyyətin müdafiəsini artırmaqdır.

Tədqiqatın predmeti, kiber hücumları və bu hücumlara qarşı mövcud olan müdafiə və fəallaşdırma strategiyalarının təhlili və qiymətləndirilməsidir. Bu predmet ətrafında, fərqli hücum növləri vardır və bu hücumlara cavab olaraq inkişaf etdirilmiş olan müdafiə tədbirləri araşdırılmalıdır.Kiber hücumlara qarşı qorunma və fəallaşdırma strategiyalarını tətbiq etməkdə məqsədimiz məsuliyyət daşıyan təşkilatların və fərdi şəxslərin məlumatların qorunmasıdır. Bu obyekt daxilində, həm dövlət təşkilatları, bank və maliyyə institutları, həm də şəxsi və müəssisələr kiber təhlükəsizlik tədbirlərinin tətbiqinə marağ göstərən paytaxt və rəhbərliklər daxildir (Garcia, 2023: 55-70).

Kiberhücumların həcmi, tezliyi və mürəkkəbliyi artmağa davam etdikcə kibermüdafiə istənilən təşkilatın kibertəhlükəsizlik strategiyasının ən ayrılmaz və çətin hissələrindən biridir. Kibermüdafiə insidentləri müəyyən etmək, təhlil etmək və hesabat vermək üçün firewall, şəbəkənin aşkarlanması və cavablandırılması (NDR), son nöqtənin aşkarlanması və cavablandırılması (EDR) kimi qoruyucu prosedurları həyata keçirməklə məlumatı, sistemləri və şəbəkələri kiberhücumlardan qoruyan əlaqələndirilmiş müqavimət aktıdır. şəbəkə daxilində baş verənlər. Yenə də kibermüdafiə komandaları təşkilatın bütün zəifliklərini təmin etmək kimi qeyri-mümkün bir vəzifə ilə üzləşirlər və bunun böyük bir hissəsi təcavüzkarların taktikalarını, imkanlarını və motivlərini dərindən başa düşmək deməkdir (Peter, Allan, 2014: 320).

Kibertəhlükəsizliyin özü nəyi əhatə edir?

1. Şəbəkə Təhlükəsizliyi

Kibertəhlükəsizlik ilk növbədə məlumatların ötürülməsi və saxlanması ilə əlaqəli olsa da, şəbəkə təhlükəsizliyi bir qədər genişdir. Adından da göründüyü kimi, şəbəkə təhlükəsizliyi ümumi şəbəkələrin qorunması, saxlanması və bərpasını əhatə edir. Kibertəhlükəsizliyi, müəyyən bir kiberhücumun məqsədi məlumatların istifadəsi ilə əlaqəli olmasa da, bütün şəbəkə istifadəçilərini bütün rəqəmsal təhdidlərdən qoruyan bir növ müdafiə kompleksi kimi əhatə edir (Bryan, 2018: 400).

2. İnformasiya təhlükəsizliyi

Dəyərli məlumatlar həqiqətən bu trafikə əsasən təhlil edilə bilər, lakin nəticədə başqa bir xidmət üst - üstə düşür-informasiya təhlükəsizliyi mütəxəssisləri birbaşa tərəfdarlardır. Bu tədqiqat sahəsi ciddi risk qiymətləndirməsini, praktik cavab strategiyalarını və fəlakətin bərpasını planlaşdırmağı əhatə edir; bu proses xüsusi uzunmüddətli qoruma planları ilə həyata keçirilir (Abbasov, 2023: 45-60).

3. Əməliyyat təhlükəsizliyi

Opsec olaraq da bilinən əməliyyat təhlükəsizliyi, risklərin idarə edilməsi prosesi olaraq modul dizaynı ilə tez-tez qiymətləndirilir. Şirkət rəhbərliyini ümumi təhlükəsizliklə əlaqəli potensial çatışmazlıqları müəyyənləşdirmək üçün iş əməliyyatlarına xarici baxımdan baxmağa çağırır. Şirkətlər ictimaiyyətlə əlaqələri idarə etməkdə üstün olsalar da, məlumat oğruları heç bir risk olmadan alt mətn şəklində məlumat toplaya bilərlər. Bu ssenaridə məlumatların oğurlanması riski daha yüksəkdir, çünki təhlil olunan məlumatlar standart təhlükəsizlik protokollarından fərqli əməliyyat məlumatları şəklində iş divarları xaricində toplanır (Johnson, 2023: 75).

4. Proqram Təhlükəsizliyi.

Tətbiq təhlükəsizlik qrupları, proqram modifikasiyası və şifrələməyə əlavə olaraq təhlükəsizlik divarına yönəlmiş müxtəlif təhlükəsizlik tədbirləri tətbiq edərək proqram kodunun oğurlanmasının qarşısını alır. Bir çox müasir tətbiq bulud əsaslı olduğundan, şəbəkəyə giriş potensial təhlükə olaraq qalır (Yanık, 2021).

Xoşbəxtlikdən, bir çox proqram təhlükəsizliyi mütəxəssisi proqram təminatından şəbəkə səviyyəli zəiflikləri aradan qaldırmaqda mütəxəssisdir.Bu hücumlar adətən məlumat oğurluğu, məlumatların manipulyasiyası, xidmətdən imtina, zərərli proqram infeksiyası və digər məqsədlərlə həyata keçirilir. Kiberhücumların bəzi ümumi növləri bunlardır (Mövludov, 2023):

1. Zərərli proqram: viruslar, troyanlar, qurdlar, fidyə proqramı və s. Zərərli proqram hədəf sistemə necə yoluxur və zərər verir.

2. Fidyə proqramı hücumları: təcavüzkarlar qurbanın sənədlərini və sistemlərini kilidləmək və ya şifrələmək üçün fidyə proqramlarından istifadə edir və onları azad etmək üçün ödəniş edirlər.

3. "Xidmətdən imtina" (DOS) hücumları: DoS hücumu hədəfi həddindən artıq istəklərlə yükləyir, normal işi dayandırır və şəbəkə və ya sistem qaynaqlarını tükəndirir.

4. Şəxsiyyət oğurluğu: təcavüzkarlar sistemlərə və xidmətlərə icazəsiz giriş əldə etmək üçün istifadəçi məlumatlarını oğurlayırlar.

5. Sosial mühəndislik: sosial mühəndislik istifadəçiləri həssas məlumatları açıqlamağa və ya təhlükəsizlik tədbirlərini atlamağa məcbur etmək üçün psixoloji manipulyasiya üsullarından istifadə edir.

6. Məlumatların manipulyasiyası: təcavüzkarlar informasiya sistemlərinə daxil olur və zərərli məqsədlər üçün məlumatları dəyişdirir, silir və ya zədələyirlər.

7. Şəbəkə hücumları: şəbəkə hücumlarına şəbəkə trafikinin monitorinqi, Paket manipulyasiyası və şəbəkə rabitəsinin kəsilməsi kimi üsullar daxildir.

8. Fərdi hücumlar: təcavüzkarlar icazəsiz giriş əldə etmək üçün sistemlərə girirlər və çox vaxt uzun müddət gözə dəymədən gizli qalırlar. Bu hücumlar ümumiyyətlə casusluq və ya uzunmüddətli məlumat oğurluğu məqsədi ilə həyata keçirilir.

Ümumiyyətlə, biz proqram səviyyəsində təhlükəsizlik prosesinə nəzər olunacaq və bu da şirkətin rəqəmsal təhlükəsizliyinin bütün sahələrinə faydalı olur. Tətbiq təhlükəsizliyinin əksəriyyəti proqram

identifikasiyası, mərkəzləşdirilmiş giriş və müntəzəm icazə yoxlamaları ilə əlaqədardır. Kibertəhlükəsizliyin idarə edilməsi şəbəkədən şəbəkəyə dəyişir. Bununla birlikdə, iş vaxtı, xüsusən ümumi məlumatların qorunması qaydalarının yenilənməsini dəstəkləmək üçün etibarlı və uyğun təhlükəsizlik tədbirlərinin inkişaf etdirilə biləcəyi sabit bir əsasdır (Smith, 2023: 40-55).

C# dilində e-ticarət kibertəhlükəsizliyinin həyata keçirilməsi həssas məlumatları qorumaq, icazəsiz girişin qarşısını almaq və e-ticarət tətbiqinizin ümumi təhlükəsizliyini təmin etmək üçün müxtəlif təhlükəsizlik təcrübələrindən və texnikalarından istifadə etməyi əhatə edir. Aşağıda C#-da e-ticarət kibertəhlükəsizliyini həyata keçirmək üçün bəzi əsas sahələr və mülahizələr verilmişdir (10):

1. Təhlükəsiz Doğrulama və Avtorizasiya (Secure Authentication and Authorization):

İstifadəçi şəxsiyyətlərini yoxlamaq üçün çox faktorlu autentifikasiya (MFA) kimi güclü autentifikasiya mexanizmlərini tətbiq edin.İstifadəçi rolları və icazələri əsasında e-ticarət platformanızın müxtəlif hissələrinə girişi idarə etmək üçün təhlükəsiz avtorizasiya üsullarından istifadə edin.

2. Məlumat Şifrələmə:

Həssas məlumatları həm VBS-də (məsələn, verilənlər bazası yaddaşı), həm də tranzitdə (məsələn, ünsiyyət üçün HTTPS/TLS istifadə edərək) şifrələyin. Şifrələmə və şifrələmə əməliyyatlarını yerinə yetirmək üçün C# dilində System. Security. Cryptography kimi kitabxanalardan istifadə edin.

3. Giriş Təsdiqləmə (Input Validation):

SQL inyeksiya, cross-site scripting (XSS) və cross-site request saxtakarlığı (CSRF) kimi ümumi veb zəifliklərinin qarşısını almaq üçün istifadəçi daxiletmələrini təsdiq edin və təmizləyin.SQL inyeksiya hücumlarının qarşısını almaq üçün Parametrləşdirilmiş sorğular və ya Entity Framework kimi ORM (Obyekt-Relational Xəritəçəkmə) kimi çərçivələrindən istifadə edin.

4. Təhlükəsiz Sessiya İdarəetmə:

İstifadəçi sessiyalarını qorumaq və sessiyanın oğurlanmasının qarşısını almaq üçün təhlükəsiz seans idarəetmə təcrübələrindən istifadə edin. Sessiyanın bitməsini həyata keçirin, uğurlu girişdən sonra sessiya identifikatorlarını bərpa edin və təhlükəsiz atributları olan kukilərdən istifadə edin.

5. Təhlükəsizlik səhvlərinin qarşısının alınması:

Təhlükəsizlik risklərini minimuma endirmək üçün veb serverlərin, verilənlər bazalarının və digər komponentlərin düzgün konfiqurasiyasını təmin edin.Məlum zəifliklər aradan qaldırmaq üçün proqram təminatından asılılıqları və kitabxanaları mütəmadi olaraq yeniləyin.

6. HTTPS/TLS tətbiq edilir:

Müştərilər və e-ticarət tətbiqiniz arasında ötürülən məlumatları şifrələmək üçün güclü TLS konfiqurasiyası ilə HTTPS-dən istifadə edin.Server tərəfi sertifikatları konfiqurasiya edin və gücləndirilmiş təhlükəsizlik üçün HSTS (HTTP Strict Transport Security) funksiyasını aktivləşdirin.

7. Ümumi Hücumlardan Müdafiə:

Kobud güc hücumlarının və avtomatlaşdırılmış bot fəaliyyətlərinin qarşısını almaq üçün sürət məhdudiyyətini və CAPTCHA tətbiq edin.Müxtəlif hücum vektorlarını azaltmaq üçün təhlükəsizlik başlıqlarından istifadə edin (məsələn, Məzmun Təhlükəsizlik Siyasəti, X-Məzmun Tipi Seçimləri, X-Çərçivə Seçimləri).

8. Müntəzəm Təhlükəsizlik Testi və Monitorinqi:

Təhlükəsizlik zəifliklərini müəyyən etmək və aradan qaldırmaq üçün müntəzəm təhlükəsizlik qiymətləndirmələri (məsələn, nüfuz testi, zəifliyin skan edilməsi) aparın.Şübhəli fəaliyyətləri və təhlükəsizlik insidentlərini aşkar etmək üçün giriş və monitorinqi həyata keçirin.

9. Təhlükəsizlik Standartlarına uyğunluq:

Müvafiq təhlükəsizlik standartlarına və qaydalarına (məsələn, ödəniş kartı məlumatlarının təhlükəsizliyi üçün PCI DSS) uyğunluğu təmin edin.Ən yaxşı sənaye təcrübələri və təhlükəsizlik qaydalarından xəbərdar olun (11).

10. İstifadəçilərin və İşçilərin Maarifləndirilməsi:

Yaxşı təhlükəsizlik təcrübələrini təşviq etmək və sosial mühəndislik hücumları riskini azaltmaq üçün istifadəçilərə və işçilərə təhlükəsizlik məlumatlılığı üzrə təlimlər keçirin.

C#-da e-ticarət kibertəhlükəsizliyini həyata keçirərkən, tətbiqinizin təhlükəsizlik vəziyyətini gücləndirmək üçün. NET çərçivəsinin və üçüncü tərəf kitabxanalarının daxili xüsusiyyətlərindən istifadə edin. Əlavə olaraq, təhlükəsizliyin inkişaf dövrünə (DevSecOps) inteqrasiyasını və kibertəhlükəsizliyə proaktiv yanaşmanı qəbul etməyi düşünün (Lock, 2021: 150-155).

Nəticə

Bu məqalədə kiberhücumlara qarşı müdafiə və təsirin azaldılması strategiyalarını müzakirə etdik. Birincisi, biz güclü təhlükəsizlik infrastrukturunun yaradılmasının vacibliyini vurğuladıq. Bu infrastruktura təhlükəsizlik divarları, güclü parollar və müntəzəm təhlükəsizlik yeniləmələri kimi tədbirlər daxil olmalıdır.

İkinci olaraq, təhlükəsizlik məsələlərinə qarşı fəal monitorinq və müdafiə strategiyalarını təşkil etmək əhəmiyyətli bir addımdır. Potensial təhlükələri aşkar etmək üçün şəbəkəni yaxından izləmək və bu təhlükələrə cavab vermək əhəmiyyətlidir.

Üçüncü olaraq, proqram təhlükəsizliyi tədbirləri əhəmiyyətli rol oynayır. Proqram təhlükəsizliyində qurulmuş proqramdan aslı olaraq şirkətin və ya fərdi şəxsin məlumatlarının qorunması, potensial təhlükələri müəyyən edilməsi həyata keçirilə bilər.

Beləliklə, kibertəhlükəsizlik strategiyasının bütövlüyü etibarlı təhlükəsizlik infrastrukturu, qabaqlayıcı monitorinq və mühafizə tədbirləri, əməliyyat təhlükəsizliyinin və proqram təhlükəsizliyinin yaradılması ilə təmin edilməlidir. Bu tədbirlər birlikdə kibertəhlükəsizlik sahəsində yaxşı nəticələr əldə etməyə kömək edəcək.

Ədəbiyyat

1. Özdemir, A. (2023). Kiber Ədəbiyyat: Texnologiya ilə Yenidən Yazılan Hekayələr. İstanbul: İthaki Yayınları, s.88-95.
2. Garcia, L. (2023). Ciberliteratura: La Revolución Tecnológica en la Literatura. Madrid: Editorial Planeta, pp.55-70.
3. Peter, W.S., Allan, F. (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know", California: O'Reilly Media, 320 p.
4. Bryan, S. (2018). "Web Application Security: A Beginner's Guide". California: O'Reilly Media, 400 p.
5. Abbasov, F. (2023). Kibernetik ədəbiyyat: texnologiya və yaradıcılıq. Bakı: Azərbaycan Kitabları, s.45-60.
6. Johnson, M. (2023). Literature in the Virtual Age: Reflections on Cybernetics, Chicago: University of Chicago Press, 75 p.
7. Yanık, M. (2021). C# 9.0 .Net 4.8 ve .Net 5.0. Ankara: Seçgin nəşrlər, 604 s.
8. Mövludov, N. (2023). Kibernetik Romanlar: Texnologiya ilə Əlaqəli İdeyalar. Bakı: Şərq-Qərb Nəşriyyat, s.30-45
9. Smith, J. (2023). Cybernetic Literature: A New Frontier. New York: Penguin Books, pp.40-55.
10. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
11. https://www.upguard.com/blog/how-cybersecurity-protects-ecommerce-companies
12. Lock, A. (2021). ASP.NET Core in Action. Shelter Island, NY: Manning Publications, pp.150-155.

Göndərilib: 21.01.2024 Qəbul edilib: 27.03.2024