PARADIGMA, No.1, 2025, səh.147-152
https://doi.org/10.30546/30015.2025.1.068

ƏSAS MƏXFİLİK TƏHDİDLƏRİ

E.Q. Həsənov, E.Y. Xəlilzadə
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Elshad.Khalilzada@student.au.edu.az

Xülasə. Məqalədə rəqəmsal dövrdə informasiya təhlükəsizliyi və məxfilik problemlərinin aktuallığı və artan risklər araşdırılır. Hər gün milyonlarla insanın şəxsi, maliyyə və səhiyyə məlumatları müxtəlif veb platformalarında saxlanılır və işlənir. İşdə "OWASP Top 10 Privacy Risks" siyahısına əsaslanaraq, əsas məxfilik təhlükələri müəyyən edilir və onların qarşısını almaq üçün "Məxfilik Təsir Dəyərləndirməsi" (Privacy Impact Assessment), risk qiymətləndirməsi, təlim proqramları, təşkilati siyasət, avtomatlaşdırılmış qayda aşkarlanması, anonimləşdirmə və icazə idarəetməsi kimi qabaqcıl tədbirlər təklif olunur.

Açar sözlər: Məxfilik təhdidləri, şəxsi məlumatların qorunması, məlumat sızması, veb tətbiq zəifliklər, SQL injection.

Giriş

Rəqəmsal mühitin sürətlə genişləndiyi bu günlərdə, şəxsi məlumatların toplanması və saxlanması yeni təhlükəsizlik çağırışlarını da özü ilə gətirir. Məxfilik pozuntuları, məlumatların icazəsiz əldə edilməsi, yayılması və dəyişdirilməsi risklərini ifadə edir. Bu risklər əsasən iki qrupa bölünür: təbii fəlakətlər və insan faktoruna bağlı təhlükələr. Təbii hadisələr nəticəsində məlumatların zədələnməsi və ya itirilməsi baş verə bilər, lakin insan faktoru ilə bağlı hücumlar – kiberhücumlar, yanlış idarəetmə və s. daha mürəkkəb və çoxşaxəlidir. Bu yazıda, həm təşkilatlar, həm də fərdi istifadəçilər üçün məxfilik risklərinin idarə olunması və təhlükəsizlik tədbirlərinin təkmilləşdirilməsi istiqamətində təkliflər təqdim olunur.

Məxfilik təhdidləri və risklər

Rəqəmsal mühitin sürətlə inkişaf etdiyi bu günlərdə şəxsi məlumatların qorunması əsas prioritetlərdən birinə çevrilib. Məlumatların toplanması, saxlanması və emal edilməsi proseslərində müxtəlif zəifliklər və təhlükə faktorları mövcuddur ki, bunlar həm fərdi istifadəçilərin, həm də təşkilatların məxfilik hüquqlarını risk altına alır. Bu bölmədə, "OWASP Top 10 Privacy Risks" siyahısına əsaslanaraq, qarşılaşa biləcəyimiz əsas məxfilik təhdidlərini və onların aradan qaldırılması üçün mümkün tədbirləri müzakirə edəcəyik.

1) Veb tətbiq zəifliklər. Bir tətbiqin düzgün şəkildə dizayn edilməməsi və ya tətbiq olunmaması, problemi aşkar etməmək və ya tez bir zamanda bir düzəliş tətbiq etməmək, məxfilik pozuntusuna səbəb ola bilər. Veb tətbiqləri, xüsusilə müxtəlif təhlükəsizlik zəifliklərinə qarşı həssasdır, bu da həssas istifadəçi məlumatlarını icazəsiz şəxslərin əlinə keçirməyə səbəb ola bilər. Məxfilik təhdidlərinə yol açan zəifliklərə, "SQL injection", həssas məlumatların sızması, zəif kimlik doğrulama və sessiya idarəetməsi, "Cross-Site Scripting" (XSS) kimi müxtəlif təhlükəsizlik boşluqları daxildir. Bu zəifliklər, məlumatların icazəsiz əldə

edilməsi, manipulyasiyası və ya sızması risklərini artıraraq istifadəçi məxfiliklərini təhdid edir.[2]

2) Operator tərəfli məlumat sızması (Operator-sided Data Leakage). İstifadəçi məlumatlarının və ya bu məlumatlarla əlaqəli hər hansı bir məlumatın icazəsiz şəxslərə sızmasının qarşısının alınmaması ilə əlaqəli bir təhlükəsizlik təhdididir.[2] Bu tip məlumat sızması, əsasən operatorların və ya xidmət təminatçılarının səhv idarəetmə, zəif təhlükəsizlik tədbirləri və ya şüurlu olmayan səhvlər səbəbindən meydana gəlir. Zəif giriş nəzarəti (access control) və ya məlumatların təhlükəsiz saxlanması ilə bağlı uğursuzluqlar nəticəsində şəxsi məlumatlar və həssas məlumatlar icazəsiz şəxslərin əlinə keçə bilər.

3) Məlumat sızmasına adekvat cavabın olmaması (Insufficient Data Breach Response). Məlumat sızması və ya məlumatın pozulması baş verdikdə, zərər çəkmiş şəxslərə (məlumat sahiblərinə) bu barədə məlumat verilməməsi və ya hadisənin səbəbinin düzəldilməsi üçün tədbir görülməməsi ilə əlaqəli bir təhlükəsizlik təhdididir. Bu, həm şüurlu, həm də qeyri-ixtiyari hadisələrdən qaynaqlana bilər və nəticədə məlumatların sızması daha da genişlənə bilər [4].

Bu cür zəiflik, aşağıdakı hallarda baş verə bilər:

- **Məlumatın təxirə salınması**: Məlumat sahiblərinə və ya müvafiq orqanlara məlumatın sızması barədə vaxtında xəbərdarlıq edilməməsi.
- **Hadisənin səbəbinin aradan qaldırılmaması**: Məlumat sızmasının səbəbi tapılıb düzəldilmədikdə, yenə də məlumatın sızması davam edə bilər.
- **Zərərin azaldılmaması**: Sızan məlumatın yayılmasını məhdudlaşdırmaq və ya qorumaq üçün tədbirlər görülməməsi.

4) Şəffaf olmayan siyasətlər, şərtlər və qaydalar (Non-transparent Policies, Terms and Conditions). Məlumatların toplanması və işlənməsi zamanı istifadəçilərin hüquqlarını qorumaq üçün təqdim olunan siyasət, şərt və qaydaların aydın və asan başa düşülən olması vacibdir. Lakin, tez-tez bu sənədlər mürəkkəb, uzun və anlaşılmaz tərzdə təqdim olunur ki, nəticədə istifadəçilər öz məlumatlarının necə istifadə olunacağı barədə kifayət qədər məlumat əldə edə bilmirlər. Bu da, məlumatların icazəsiz və gözlənilməz şəkildə emal edilməsinə, istifadəçinin şəxsiyyət və məxfiliyinin risk altına alınmasına gətirib çıxara bilər.

5) Razılığın sui-istifadəsi (Consent on everything). Bu problem, məlumatların işlənməsi üçün istifadəçidən alınan razılığın, hər bir konkret məqsəd üçün ayrılıqda verilməməsi və ümumi, geniş şəkildə toplanması halında meydana gəlir. Yəni, təşkilatlar bütün fəaliyyətlər üçün vahid bir razılıq tələb edir, beləliklə istifadəçi hansı konkret məqsədlər üçün məlumatının istifadə olunacağını dəqiq bilmir. Nəticədə, istifadəçilər məlumatlarının necə və hansı şərtlər daxilində emal olunacağı barədə tam məlumat almadan razılıq vermək məcburiyyətində qalır və bu da onların gizlilik hüquqlarını zəiflədə bilər.

6) Şəxsi məlumatların vaxtında silinməməsi (Insufficient Deletion of Personal Data). Toplanmış şəxsi məlumatlar müəyyən bir məqsəd üçün istifadə edilir. Əgər həmin

məqsəd həyata keçirildikdən sonra və ya istifadəçinin məlumatların silinməsini tələb etdiyi halda bu məlumatlar vaxtında və düzgün şəkildə arxivdən çıxarılmırsa, bu, icazəsiz istifadə və məxfilik pozuntularına yol açа bilər. Bundan əlavə, belə hallar müvafiq qanunvericilik tələblərinin, məsələn, GDPR-də nəzərdə tutulan "unutulma haqqı" prinsipinin pozulmasına gətirib çıxara bilər. Buna görə təşkilatlar şəxsi məlumatların saxlanma müddətini dəqiq müəyyənləşdirərək, məlumatların vaxtında və etibarlı şəkildə silinməsi üçün effektiv prosedurlar tətbiq etməlidirlər.

7) Yetərsiz məlumat keyfiyyəti (Insufficient Data Quality). Yetərsiz məlumat keyfiyyəti, istifadəçilərin məlumatlarının güncəlliyinin, düzgünlüyünün və etibarlılığının təmin olunmadığı hallar üçün istifadə olunur. Bu risk, köhnəlmiş, səhv və ya etibarsız məlumatların istifadəsi ilə özünü göstərir və məlumatların vaxtında yenilənməməsi və ya düzəldilməməsi hallarında daha da güclənir.

Bu problemin yaranmasına bir neçə faktor təsir edir. Məsələn, məlumatların toplanması prosesində aydın olmayan təlimatlar və qeyri-dəqiq forma sahələri istifadəçilərin yanlış məlumat daxil etməsinə səbəb ola bilər. Həmçinin, məlumatların yaddaşa yazılması və giriş prosesləri zamanı baş verən texniki səhvlər nəticəsində də səhv və ya natamam məlumatlar əldə edilir. Üstəlik, məlumatların düzgün əlaqələndirilməməsi – məsələn, cookie səhvləri və ya kontakt siyahısının və ya sosial şəbəkə hesabının daxil edilməsi zamanı yaranan uyğunsuzluqlar – əlavə problemlərə yol açа bilər.

Bu cür hallar, məlumatlara əsaslanan qərarların səhv olmasına və həmçinin tənzimləyici tələblərin pozulmasına gətirib çıxara bilər. Buna görə də, təşkilatlar məlumatların düzgünlüyünü və aktual olmasını təmin etmək üçün müntəzəm yoxlama, yeniləmə və təsdiqləmə proseslərini tətbiq etməlidirlər.

8) Sessiyanın vaxtında bitməməsi və ya düzgün sonlandırılmaması. Bu vəziyyətdə istifadəçi sessiyası düzgün vaxtda başa çatdırılmır və ya heç bir zaman bitmir [3]. Nəticədə, bir sıra problemlər ortaya çıxa bilər.

İlk olaraq, sessiya oğurluğu baş verə bilər; bu,kiberhücumçuların istifadəçinin sessiya identifikatorunu oğurlayaraq, onun hesabına icazəsiz giriş etməsinə şərait yaradır. Nəticədə şəxsi məlumatlar təhlükəyə düşə bilər. İcazəsiz məlumat toplama baş verə bilər, çünki sessiya hələ aktiv olduğu üçün istifadəçi məlumatları onun xəbəri olmadan toplanmağa davam edə bilər. Məxfiliyin pozulması da mümkündür, çünki bu, istifadəçinin razılığı olmadan məlumatların toplanmasına gətirib çıxara bilər.

9) İstifadəçilərin məlumatlara əlçatanlıq və düzəliş imkanlarının olmaması. İstifadəçilərin şəxsi məlumatlarına asanlıqla baxa, onları yeniləyə və ya dəyişdirə bilməsi onların məlumat üzərində tam nəzarətini təmin edir. Lakin, əgər sistem istifadəçilərə bu imkanları təqdim etmirsə, onların şəxsi məlumatları üzərində nəzarətin itirilməsi ilə yanaşı, GDPR kimi tənzimləyici qaydaların pozulması riski də artır. Belə məhdudiyyətlər şəxsiyyət oğurluğu, məlumatların sızması və fərdi məxfilik hüquqlarının zədələnməsi kimi təhlükələrə

yol açır. Nəticədə, istifadəçilər öz məlumatlarını idarə edə bilmədikdə, icazəsiz giriş və ya üçüncü tərəflərlə məlumatların paylaşılması riski də yüksəlir [2].

10) İstifadəçinin razılığına uyğun olmayan məlumatların toplanması (Collection of data not required for the user-consented purpose). Sistemlərin işləmə məqsədləri üçün istifadəçinin açıq şəkildə razılıq verdiyi məlumatlardan kənar əlavə məlumatların toplanması ciddi risklər yaradır. Məsələn, istifadəçilərin demoqrafik, təsviri və ya digər əlaqəli məlumatlarının, sistemin əsas funksionallığı üçün zəruri olmadığı halda toplanması, onların şəxsi məlumat hüquqlarının pozulmasına səbəb ola bilər. Bu cür məlumatların icazəsiz emalı, istifadəçinin şəffaf razılığı olmadan həyata keçirildiyi üçün həm hüquqi, həm də etik öhdəliklərin pozulmasına yol açır. Nəticədə, əlavə məlumatların yığılması istifadəçinin şəxsi məlumatlarının icazəsiz istifadə olunması, təhlükəsizlik pozuntuları və məlumat sızması kimi riskləri artırır. Təşkilatlar, yalnız istifadəçinin açıq razılığına əsaslanan və sistemin işləmə məqsədlərinə uyğun məlumatları toplamağa diqqət yetirməli, lazımsız məlumatların toplanmasının qarşısını almaq üçün ciddi nəzarət mexanizmləri tətbiq etməlidirlər.

Məxfilik təhdidlərinə qarşı müdafiə: tədbirlər və yanaşmalar

Məxfilik təhdidlərinin qarşısını almaq üçün qabaqcıl tədbirlərin həyata keçirilməsi vacibdir. Bir sıra təhlükəsizlik tədbirləri aşağıda qeyd olunmuşdur:

1) Məxfilik Təsir Dəyərləndirməsi (Privacy Impact Assessment - PIA). Bu, hər hansı bir yeni sistem və ya proses tətbiq olunmadan əvvəl məlumatların işlənməsinin məxfiliyinə təsirlərini analiz etmək üçün aparılır. PIA həm də riskləri müəyyən etməyə və onları minimuma endirmək üçün planlar hazırlamağa kömək edir [2].

2) Cari tətbiq portfelində risk qiymətləndirilməsi. Təşkilatın istifadə etdiyi bütün proqram təminatlarında məxfiliklə bağlı risklərin qiymətləndirilməsi aparılır.

3) Məxfiliklə bağlı təlimlər. Rəhbərlər, işçilər və istifadəçilər üçün məxfiliklə bağlı təlimlərin keçirilməsi nəticəsində məxfiliklə bağlı məlumatlılıq artır, səhvlərin və zərərli davranışların qarşısını alır.

4) Təşkilati məxfilik siyasəti. Təşkilatın bütün işçiləri üçün məxfilik standartlarının təsbit edilməsi və yazılı şəkildə təqdim edilməsidir. Bu, təşkilat daxilində vahid məxfilik mədəniyyətinin formalaşdırılmasını təmin edir.

5) Məxfilik tələblərinin avtomatik aşkarlanması. Proseslərin avtomatlaşdırılması yolu ilə məxfilik qaydalarına əməl olunmasını təmin edir. İnsan səhvlərini azaltmağa və məlumatların təhlükəsizliyini artırmağa kömək edir**.**

6)Anonimləşdirmə və Psevdonimləşdirmə. Məlumatların istifadəçilərin şəxsiyyətini aşkar etməyəcək şəkildə dəyişdirilməsidir. Bununla istifadəçi məlumatlarının təhlükəsizliyi artır və məxfiliyi qorunur [2].

7) İcazələrin düzgün idarə edilməsi. Şəxsi məlumatların qorunması və istifadəçi etibarının təmin edilməsi üçün əsas rol oynayır. Bu, istifadəçilərdən məlumat toplanmadan

əvvəl onların açıq və məlum olan icazəsini almayı, yalnız müəyyən məqsədlər üçün məlumatları istifadə etməyi və istifadəçilərə icazələrini istənilən vaxt dəyişdirmə və ya geri götürmə imkanı verməyi əhatə edir.

8) Məlumatların minimalizasiyası və saxlanma qaydaları. Toplanılan məlumatların yalnız sistemin işləmə məqsədləri üçün zəruri olan hissəsini əhatə etməsi və müəyyən edilmiş müddətdən sonra avtomatik silinməsi təşkilatların risklərini azaldır. Bu yanaşma, lazımsız məlumatların saxlanmasının qarşısını alaraq, potensial icazəsiz istifadə və məlumat sızması hallarını minimuma endirir.

9) Güclü giriş nəzarəti və şifrələmə tədbirləri. İstifadəçi məlumatlarının həm ötürülmə, həm də saxlama mərhələsində şifrələmə mexanizmlərinin tətbiqi, məlumatların icazəsiz əldə olunmasının qarşısını alır. Eyni zamanda, ciddi giriş nəzarəti vasitələri ilə yalnız səlahiyyətli şəxslərin məlumatlara daxil olmasına icazə verilməsi təmin edilməlidir.

10) Davamlı təhlükəsizlik auditi və monitorinq. Məlumatların işlənməsi və saxlanması proseslərində müntəzəm audit və real vaxt monitorinqi aparılmalıdır. Bu tədbir, potensial zəiflikləri vaxtında aşkar etməyə və onların dərhal aradan qaldırılmasına şərait yaradır.

11) Hadisələrə cavab və bildiriş planı. Məlumat sızması və digər təhlükəsizlik hadisələri baş verdikdə, təşkilatın tez və effektiv müdaxilə edə bilməsi üçün konkret cavab planı hazırlanmalıdır. Bu plan, həm istifadəçilərin, həm də müvafiq nəzarət orqanlarının hadisədən dərhal xəbərdar edilməsini təmin etməlidir.

12) Məxfi dizayn və tətbiqində əsas prinsiplər. Yeni sistem və proseslərin yaradılması zamanı "privacy by design and by default" yanaşmasının tətbiq edilməsi vacibdir. Məxfilik prinsipləri ilkin mərhələdən etibarən nəzərə alınaraq, istifadəçi məlumatlarının qorunması əsas prioritet kimi müəyyənləşdirilməlidir.

Nəticə. Bu məqalədə müasir cəmiyyətdə şəxsi məlumatların qorunmasının və məxfilik təhdidlərinin idarə olunmasının əsas aspektləri geniş şəkildə araşdırılıb. Məlumat sızması, veb tətbiq zəifliklər (SQL injection, Cross-Site Scripting və s.), operator tərəfli məlumat sızması və sessiya idarəetməsindəki çatışmazlıqlar kimi risklər, istifadəçi məlumatlarının icazəsiz əldə olunmasına və manipulyasiyasına yol açır. Bu problemlərin həllində şəffaf siyasətlər, istifadəçi razılığı, GDPR tələblərinə riayət, Privacy Impact Assessment (PIA) və risk qiymətləndirilməsi kimi tədbirlərin tətbiqi vacibdir. Həmçinin, məxfiliklə bağlı təlimlər, anonimləşdirmə, psevdonimləşdirmə və icazələrin düzgün idarə edilməsi kimi yanaşmalar təşkilatların və fərdi istifadəçilərin məlumat təhlükəsizliyini artırmağa kömək edir. Nəticə etibarilə, davamlı inkişaf və innovativ yanaşmaların tətbiqi, rəqəmsal mühitdə məlumatların müdafiəsini təmin etməklə, ictimai etibarın və hüquqi öhdəliklərin qorunmasına mühüm töhfə verir.

Ədəbiyyat

1. Martin, K. (2016). *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*.
2. OWASP. (2022, May 30). *OWASP Top 10 Privacy Risks Countermeasures v2.0*. The Open Web Application Security Project
3. OWASP. (n.d.). *Session Management Cheat Sheet*.
4. Privacy Patterns. (n.d.). *Data breach notification pattern*

MAJOR PRIVACY THREATS

E.G. Hasanov, E.Y. Khalilzade
Azerbaijan University, Jeyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. This article highlights the relevance and increasing risks of information security and privacy issues in the digital age. Every day, the personal, financial, and healthcare data of millions of people are stored and processed on various web platforms. Based on the "OWASP Top 10 Privacy Risks" list, the article identifies the main privacy threats and proposes advanced measures such as *Privacy Impact Assessment*, risk evaluation, training programs, organizational policies, automated rule detection, anonymization and access control to mitigate them.

Keywords: Privacy threats, personal data protection, data leakage, web application vulnerabilities, SQL injection.