

Sosial şəbəkələrdə gizlilik və təhlükəsizlik problemləri

Nərgiz Abdullayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

nargiz.ni.21@gmail.com

Xülasə — Bu məqalədə onlayn sosial şəbəkələrdə gizlilik və təhlükəsizlik problemləri analiz edilmişdir. Sosial şəbəkə riskləri və onlardan qorunmağın yolları araşdırılmışdır.

Açar sözlər - onlayn sosial şəbəkələr; gizlilik riskləri; data mining,

I. GİRİŞ

Hal-hazırda onlayn sosial şəbəkələr internet mühitində fəaliyyət göstərən ən təsirli media quruluşlarından biri halına gəlmişdir. Sosial media İnternet texnologiyaları vasitəsilə insanlar arasında virtual sosial ünsiyyət yaratmaq və məlumatları paylaşma deməkdir. O, daha əlçatan və veb əsaslı texnologiyalardan istifadə etməklə ünsiyyəti interaktiv dialoqa çevirir. Sosial media vasitələrinə internet üzərindən yayımlanan informasiya saytları, sosial şəbəkələr, bloqlar, mikro bloqlar, ani ünsiyyət proqramları, forumlar daxildir. Sosial şəbəkələr bizim fiziki dünyamızın virtual formasıdır [1]. Onlayn sosial şəbəkələr istifadəçilərə zaman və məkan məhdudiyyəti qoymadan bir çox imkanlar təklif edir. Son illərdə onlayn sosial şəbəkə istifadəçilərində və mövcud məlumatların sayında hədsiz artım müşahidə edilir. Onlayn sosial şəbəkələrin yayılması ilə bu şəbəkələrdə informasiya mübadiləsi də daim artan əhəmiyyətə malikdir. Onlayn sosial şəbəkələr əhalinin böyük segmentinin həyatının daimi iştirakçısıdır və offlayn fəaliyyətlərinə də birbaşa təsir göstərir. Əlbəttə ki, bu da ciddi gizlilik və təhlükəsizlik riski yaradır.

Bu məqalədə sosial şəbəkə məlumatlarına diqqət yetirilib və məlumatların toplanmasına və qorunmasına dair problemlər aşkarlanıb. İstifadəçilərin gizlilik və təhlükəsizliyinin qorunması üçün istifadə olunan bir sıra mövcud üsullar və sosial şəbəkə problemləri araşdırılıb, təkliflər verilib.

II. SOSIAL ŞƏBƏKƏLƏRDƏ GİZLİLİK VƏ TƏHLÜKƏSİZLİK RİSKLƏRİ

Sosial şəbəkələr bir çox şəxsəndən ibarət ekosistemdir [2]. Gizlilik və bir şəxsin sosial şəbəkəsi arasındakı əlaqə çox yönlüdür. Gizlilik siyasətinin sosioloji nəzəriyyələri fərdlərin fərqli dərəcədə inam və yaxınlıq yaratmaq üçün başqaları ilə fərdi məlumatları paylaşmağı necə seçə biləcəyini qeyd edir [3].

Gizlilik və təhlükəsizliyin möhkəmləndirilməsi ilə bağlı olan unikal problemləri anlamaq üçün ilk növbədə şəbəkə

təhlükəsizliyinin standart prinsiplərini, o cümlədən onların onlayn sosial şəbəkələr üçün necə genişləndirildiyini nəzərdən keçirməliyik. Daha sonra, xüsusilə istifadəçilərin fərdi məlumatların aşkar etmək üçün sosial şəbəkə analizi və əlaqəli üsulları üzərində gizlilik və təhlükəsizlik hücumlarının necə qurulacağına baxılır.

Gizlilik onlayn sosial şəbəkələrdə mühüm əhəmiyyət kəsb edir. Çünki istifadəçilərin şəxsi məlumatlarının qeyri-qanuni açıqlanması və düzgün istifadə edilməməsi insanların həyatında istənməyən və zərərli nəticələrə səbəb ola bilər. Onlayn sosial şəbəkələr çərçivəsində gizlilik bir neçə geniş kateqoriyaya malikdir:

- İstifadəçi şəxsiyyətinin gizliliyi – müxtəlif onlayn sosial şəbəkələr arasında istifadəçinin şəxsiyyətinin qorunması;
- İstifadəçinin fərdi gizliliyi – bura istifadəçinin biblioqrafik məlumatları, şəxsi dosyaları və s. daxildir;
- İstifadəçinin ünsiyyət gizliliyi - bura əlaqələrin vaxtı və uzunluğu, əlaqələrin yeri (IP ünvan), digər istifadəçi profillərinə göndərilən və alınan məktublar və s. [4] daxildir;

Bəzən biz özümüz haqqında məlumatı kənar şəxslər tərəfindən deyil, yalnız dost qrupları ilə paylaşmaq istəyirik. Bunun üçün onlayn sosial şəbəkələrdə gizliliklə bağlı “xəbərdarlıq və razılıq” xidməti fəaliyyət göstərir. Bu yanaşma xidmətin məxfilik praktikasını istifadəçiyə bildirir və istifadəçi xidmətə daxil olub-olmamasını seçir. Lakin bəzi hallarda sosial şəbəkələrdə gizlilik istifadəçi tərəfindən pozulur. Və bu pozuntular sosial şəbəkələrdə kimlik oğurluğu və ya məlumatların sızması, spam profillərdən saxta istəklər, ictimai paylaşma riskləri, saxta təbiiqlər və zərərli linklər kimi bir sıra riskləri gətirib çıxarır. Bu risklərə qısaca nəzər yetirək:

1) *Kimlik oğurluğu*: Buna sosial şəbəkələrdə saxta profillər də deyilir. 2012-ci ildə 12 milyon insan kimlik oğurluğu və məlumat sızmasının qurbanı olmuşdur. Bu hadisə ABŞ-da *müştərilərin* məxfi məlumatlarını idarə edən maliyyə təşkilatlarının ümumilikdə təxminən 21 milyard dollar pul itkisinə səbəb olmuşdur.

2) *Sosial paylaşım riski*: Facebook, Snapchat, Instagram kimi geniş yayılmış ictimai sosial şəbəkələrdə fotoşəkillər ilə yanaşı mövcud yerləri paylaşa bilən xüsusiyyət var. Bu

yerlər ərtaflı ünvan şəklində göstərildiyi üçün istənilən şəxs sizi tapmasını asanlaşdırır.

3) *Saxta tətbiqlər və zərərli linklər*: Sosial şəbəkələrdə saxta tətbiqlər və linklər mövcuddur. İstifadəçi həmin linkə daxil olduqda onun mobil nömrəsi, e-mail ünvanı və s. kimi şəxsi məlumatları həmin tətbiqlər tərəfindən oğurlana bilər.

Bəs bu risklərin qarşısını almaq, onlardan qorunmaq üçün nə etmək olar? Onlayn sosial şəbəkələrdə gizlilik və təhlükəsizlik risklərində qorunmaq üçün aşağıdakı məsləhətləri təklif edirik.

- Güclü şifrə yaradın. Ad, doğum tarixi, telefon nömrəsi kimi məlumatları şifrələmədə istifadə etməyin. Daha çox rəqəmdən, böyük hərflərdən, fərqli simvollarından istifadə edin. Şifrəniz nə qədər güclü olsa risk daha az olacaq.
- Sosial profillərinizi tez-tez nəzərdən keçirin və hər bir şəxsi məlumatların qorunmasına diqqət yetirin. Sosial şəbəkələrin gizlilik xidmətlərinə riayət edin.
- Saxta tətbiqlər və zərərli ola biləcək linklərə daxil olmayın. Bunlar həm virus, həm də kiberterrorizm xarakterli ola bilər.
- Gələn mesajların və sorğuların bloklanması kimi sosial şəbəkə tərəfindən təklif olunan genişləndirilmiş gizlilik seçimlərindən istifadə edin və s.

NƏTİCƏ

Sosial şəbəkələrdə şəxsi məlumatların əldə edilməsinə nəzarət və onun mühafizəsinin təmin olunması üçün onlayn sosial şəbəkələr bir sıra daxili nəzarət mexanizmlərinin istifadəsini dəstəkləyir [5,6]. Lakin onlayn sosial şəbəkə istifadəçilərinin tədqiqatları nəticəsində ortaya çıxır ki, bu mexanizmlər profillərin və şəxsi məlumatların qorunmasına tam müvəffəq ola bilmir [7]. Onlayn sosial şəbəkə xidmətlərini optimallaşdırmaq və istifadəçilərin üstünlükləri və maraqları baxımından fərdləşdirmək üçün Data Mining texnologiyalarından istifadə edilə bilər. Bununla belə, sosial Data Mining və onlayn sosial şəbəkələrin tələbləri arasında potensial münaqişələr yarana bilər. Hər hansı bir rəqib sosial şəbəkə istifadəçilərinin gizlilik parametrləri ilə nəşr olunan

sosial şəbəkə məlumatlarını və bəzi başqa məlumatları istifadə edərək daxil ola bilər. Buna görə də onlayn sosial şəbəkələrin gizlilik tələblərinə cavab vermək üçün qraf anonimləşdirmə proseduruna daxil edilməlidir. Aydındır ki, Data Mining nəticələri və onlayn sosial şəbəkə istifadəçilərinin gizlilik tələbləri arasında qarşılıqlı əlaqə var. Ədəbiyyatlarda bir çox qraf anonimləşdirmə üsulları təklif olunmasına baxmayaraq, bu praktikada hələ də məhduddur.

ƏDƏBİYYAT

- [1] R.M.Alıquliyev, N.Ə.İsmaylova., “Sosial mediada milli informasiya təhlükəsizliyinə təhdidlərin aşkarlanması üçün yanaşma,” İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi-praktiki seminarı, 2017, pp. 70-72
- [2] I. Kayes, A. Iamnitchi., “Privacy and security in online social networks: A survey,” Online Social Networks and Media, Vol. 3–4, 2017, pp. 1–21
- [3] Lipford H.R., Besmer A., Watson, J., “Understanding privacy settings in facebook with an audience view,” Proceedings of the 1st Conference on Usability, Psychology, and Security, 2008, pp. 1–8.
- [4] R. Gross, A. Acquisti, “Information Revelation and Privacy in Online Social Networks,” Workshop on Privacy in the Electronic Society (WPES), 2005, pp. 71-80.
- [5] Liu Y., Gummadi K.P., Krishnamurthy B., Mislove A., “Analyzing facebook privacy settings: user expectations vs. Reality,” Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. (IMC '11), 2011, pp.68–73.
- [6] Johnson M., Egelman S., Bellovin S.M., “Facebook and privacy: it's complicated,” Proceedings of the Eighth Symposium on Usable Privacy and Security. (SOUPS '12), 2012, pp. 1–15.
- [7] C. Zhang, J. Sun, X. Zhu, Y. Fang, “Privacy and Security for Online Social Networks: Challenges and Opportunities,” IEEE Communications Society, 2010, pp. 13-18.

PRIVACY AND SECURITY ISSUES ON SOCIAL NETWORKS

Nargiz Abdullayeva

Institute of Information Technology of ANAS,

Baku, Azerbaijan

Abstract -- This article analyzes privacy and security issues in online social networks. Social network risks and ways of protection are studied.

Keywords -- online social networks; privacy risks; data mining