SOCIAL NETWORKS AND DIGITAL SECURITY

Mihaela A. Karadocheva [1], Ekaterina M. Konstantinova [2], Albena B. Aleksandrova [3]

[1] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", mkaradocheva6@gmail.com
[2] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com
[3] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Management of Security Systems", alb.alexandrova@abv.bg

***Abstract**: The social networks become more and more frequently used and there are many users all around the world. The social media helps us to connect with each other and make new friends, share everything we want with them, but there are some risks that every user should have in mind and should know how to avoid being a victim of all the possibilities of the Internet.*

***Keywords**: Cyber security, Digital security, Internet, Social networks*

СОЦИАЛНИ МРЕЖИ И ДИГИТАЛНА СИГУРНОСТ

Михаела А. Карадочева, Екатерина М. Константинова, Албена Б. Александрова

1. Въведение

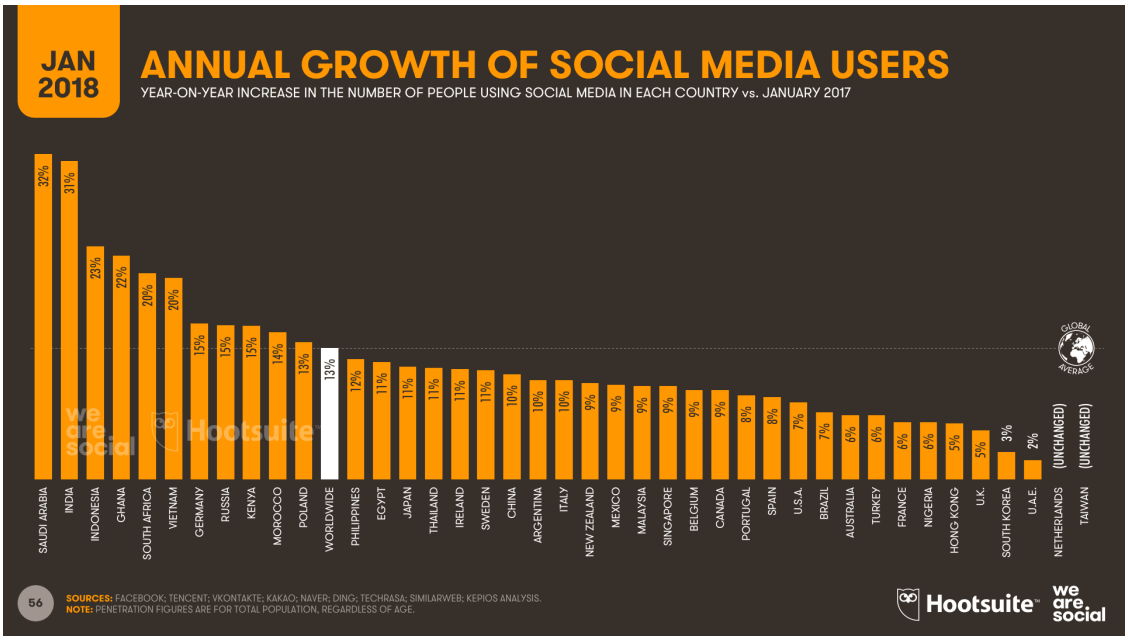
Кибер престъпленията днес са глобален проблем, който се отразява върху много сфери на нашия живот. Почти всичко, което виждаме в нашето ежедневие, вероятно има нужда от кибер-сигурност. Дори когато се разхождаме в парка, наоколо има камери и много дигитални устройства, които могат да бъдат използвани срещу нас, ако за тях не се грижат всеки ден специалисти, повишаващи непрекъснато защитата им. Уязвимостта от дигиталния свят не трябва да причинява параноя, но всеки, който използва привилегиите на модерното време, трябва да знае основите на дигиталната сигурност [1], [2], [5], [8], [9], [12], [13], [14], [15], [16], [21].

2. Изложение

Социални мрежи като Facebook, Instagram и Twitter се разрастват много в последните години. Те позволяват на хората да общуват с техните контакти, да възобновят отношения със стари познати, да създадат нови връзки с други хора, базирани на общи хобита, интереси и кръгове от хора. През последните години се наблюдава огромен ръст в използването на социалните мрежи, като общо се събира информация за над половин милиард регистрирани потребители (Фиг. 1). Като резултат, социалните мрежи съхраняват огромно количество лична информация за потреби-

телите и техните действия. Популярността на социалните мрежи привлича не само честни потребители, но и други лица, имащи по-различни намерения. Неизбежен е риска от нарушаване на поверителността на всички потребители в резултат на обмена на информация и споделянето в Интернет [1], [2], [5], [17], [18], [19], [20].

Независимо от идеята на социалните мрежи, една от главните причини за потребителите да се регистрират, създадат профил и да използват различни приложения е възможността лесно да споделят информация с определени контакти или публично. Разкриване на лична информация в интернет пространството е опасно, тъй като това може да доведе до злонамерени атаки в реалния и интернет световете като преследване, клеветене, имейл спам и други. Независимо от рисковете, много от контролните механизми за достъп и поверителност са умишлено отслабени, за да направят лесно присъединяването към социална мрежа и споделянето на информация.



Фигура 1: Ръст в използването на социални мрежи за 1 година – януари 2017 г.-януари 2018 г.

Има голямо разнообразие измежду социалните мрежи. Всеобщо прието е, че всички те споделят едни и същи основни свойства. Социалната мрежа е дигитално представяне на нейните потребители и техните социални връзки във физическия или виртуалния свят, плюс услуги за съобщения и социализиране между потребителите. Предоставя се платформа за:

- Позволяване на потребителите да създадат дигитално представяне на себе си (обикновено познато като потребителски профили);
- Поддръжката и подобряването на вече съществуващите социални връзки между потребителите във физическия или виртуалния свят;
- Създаване на нови връзки, базирани на общи интереси, локация, дейности и т.н.

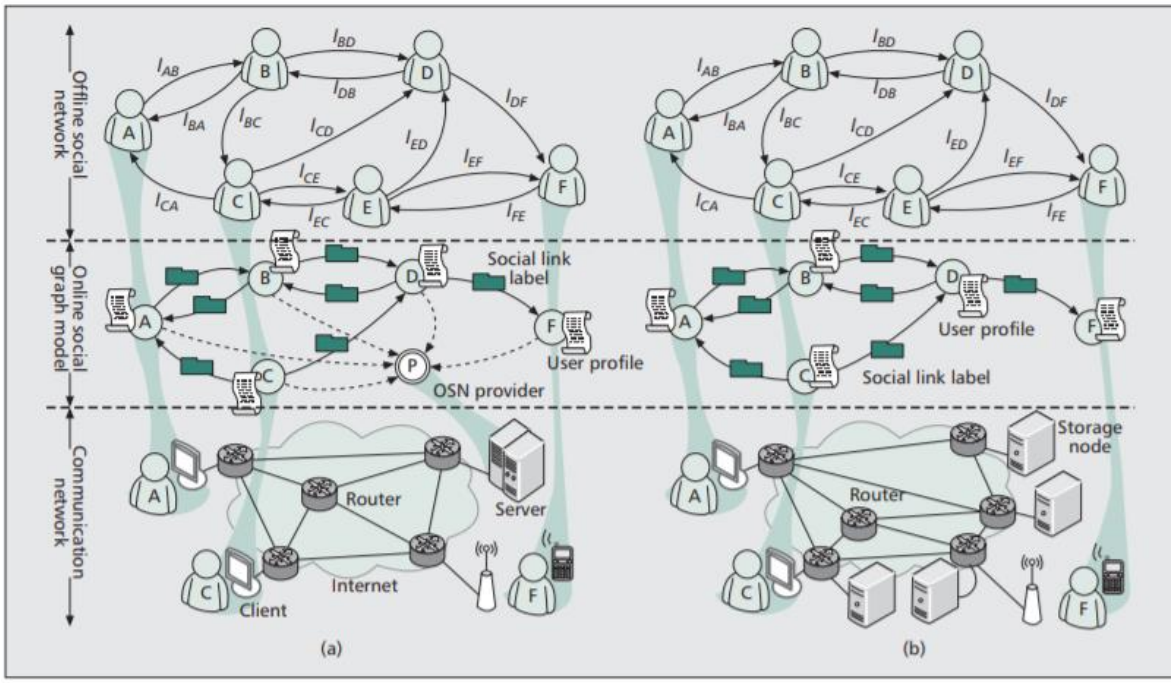
Има две парадигми за имплементирането на социална мрежа в литературата – клиент-сървър архитектура и peer-to-peer архитектура (P2P).

Днешните социални мрежи са централизирани и базирани на уеб-сървър. Всички функционалности като съхранение, поддръжка и достъп до социалните услуги се предлагат от комерсиални доставчици като Facebook Inc. и LinkedIn Corp. Тази традиционна архитектура има предимството да бъде проста и лесна за имплементиране, но страда от недостатъците на централизираните системи [1], [3], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16].

За следващите поколения социални мрежи съществува тенденцията за използване на P2P архитектура, която е децентрализирана архитектура, разчитаща на сътрудничество между няколко независими участници, които също са потребители на социални мрежи. Информацията за раз-

личните потребители се съхранява отделно. С поддържането на директен обмен на информация между устройства, било то между потребители, които вече са се срещали, или между съседни възли в градската мрежа, P2P архитектурата се възползва от предимството на реалните социални връзки и географската близост, за да поддържа локални услуги, когато не е наличен достъп до Интернет.

Фигура 2 илюстрира двата вида архитектури за социална мрежа, където клиент-сървър архитектурата (a) изисква Интернет връзка, за да могат потребителите на комуникират чрез отдалечен централен сървър, а P2P архитектурата (b) поддържа комуникация чрез локална връзка, тъй като ролята на централния сървър е разпределена във всеки възел за съхранение [2], [4], [8].



Фигура 2: Архитектури на социалните мрежи. a) Клиент-сървър; b) P2P

Поверителността е от първостепенно значение за социалните мрежи, тъй като незаконното разкриване и неправилното използване на личната информация на потребителите може да причини нежелани или вредни последици в живота на хората. Поверителност в контекста на социалните мрежи има няколко категории:

Анонимност на потребителя

Защитата на идентичността на потребителя се променя според различните типове социални мрежи. В сайтове като Facebook използването на истински имена за представяне на профила е препоръчително. Няма анонимност на идентичността, защото повечето приложения във Facebook разчитат на връзка на профилите с техните публични идентичности. В сайт за срещи като Friendster е видимо само първото име на потребителя. В уеб сайтове за запознанства, базирани на псевдоними, не се подкрепя използването на лична информация.

Поверителност на личното пространство на потребителя

Видимостта на потребителския профил също варира в зависимост от различните типове социални мрежи. Има сайтове, където профилите са видими за всички и участват в търсачките. Други сайтове имат опцията потребителя да избира дали профилът му да бъде видим публично или само за приятели [2], [4], [7], [8], [9], [17], [18], [19], [21].

Поверителност на комуникацията на потребителя

В допълнение към личните данни, разкрити в дигиталното пространство на потребителя, той може също да разкрие лична информация на мрежовия оператор или доставчика на социална

мрежа: данни като време и дължина на връзката, местоположение (IP адрес) на връзка, посетени профили, изпратени и получени съобщения и т.н.

Всички данни, получени от потребителите, се съхраняват в различни таблици и графики. Най-често атаките са насочени към тези таблици, като биват два типа – подправяне на идентичност и подправяне на връзки [4], [8], [9], [17], [19], [20]. Подправянето (кражбата) на идентичност е фундаментален проблем в социалните мрежи и лежи в основата на много други усложнения, свързани със сигурността. Например зложелател може да направи фалшив профил на известна личност или марка, за да печели от тяхната репутация. Всеки потребител трябва да бъде сигурен в самоличността на отсрещния, за да бъде в безопасност от кибератака.

Улесняването на социалните взаимоотношения е главната функция на социалните мрежи. Въпреки това е възможно неконтролируемо изтичане на информация на потребителите. Събраните данни от доставчиците на социални мрежи са важен източник за социални и маркетинг проучвания, които могат да предоставят полезна информация за развитието и еволюцията на социалното общество. Също така могат да бъдат използвани за оптимизиране на услугите на социалните мрежи и настройването им според потребителските предпочитания и интереси. Въпреки това съществува потенциален конфликт между събирането на данни и изискванията за поверителност. Евентуален неприятел може да използва публикувани данни от социални мрежи и благодарение на някои основни познания да наруши поверителността на потребителя. Дори след скриване на идентичността посредством заменяне на имената със случайни безсмислени идентификатори, е доказано, че базирано на графики с топологична информация, е възможно разкриването на самоличността на повечето потребители. Следователно, за да отговарят на изискванията за поверителност на социалните мрежи, графиките трябва да съдържат несъответствия. Очевидно е налице компромис между качеството на резултата от извличане на данни и изискванията за поверителност.

Заключение

Социалните мрежи са голяма част от ежедневието на днешния човек. Всеки трябва да е наясно с рисковете на интернет пространството и какви опасности крие то, както и да знае начините за предпазване на своята идентичност и лични данни [3], [9].

References

1. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на Киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни", Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.

2. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.

3. Парашкеванова, Г., Цанков, Ц. (2016). *Киберпрестъпността като основна съвременна заплаха за големите организации*. Научна конференция MATTEX 2016, Шумен, ISSN 1314-3921.

4. Стаменова, А., Диманова, Д., Цанков, Ц. (2014). *Новите войни на XXI век*. Научна конференция MATTEX 2014, Шумен, ISSN 1314-3921.

5. Nikolov, L., Slavyanov, V. (2018). *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, ISSN 2367-7902.

6. Yankova-Yordanova, Y., Dyankov, P. (2016). *Automated systems for process control*. International scientific refereed online journal publisher:"Smart ideas – wise decisions" Ltd., Bulgaria, ISSN 2367-5721, issue 27.

7. Yankova-Yordanova, Y., Tsankov, Ts. (2019). *Opportunities for Remote Use a Powerful Computer*. Journal of Physics and Technology, Plovdiv university press “Paisii Hilendarski”, Plovdiv, ISSN 2535-0536.

8. URL: https://www.aresearchguide.com/30-cyber-security-research-paper-topics.html

9. URL: https://pdfs.semanticscholar.org/08fa/0252365bda9bf7ea5b70a48dd4f744519fed.pdf

10. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.

11. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.

12. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.

13. Boyanov, P., *Unauthorized access attempts to the information resources of private computer networks in academic institutions via network scanning cyber attacks,* Yearbook of Higher School of Security and Economics, Plovdiv, Publishing complex HSSE, ISSN 2367-8798, Vol. XV, 2018, c. 51-58.

14. Боянов, П., *Приложение на кибератаката от тип социално инженерство срещу правителствени агенции, частни организации и академични институции*. Сборник научни трудове - Научна конференция с международно участие "MATTEX 2018" - 25-27 октомври 2018, ISSN: 1314-3921, т.2, ч.1, 2018, с.42-51.

15. Boyanov, P., Tasheva, Zh., Fetfov, Og., Trifonov, T., Uzunova, B., *Securing the social profiles from malicious and unauthorized access*, Proceedings of the 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2014), Liepaya, Latvia, ISBN 978-9934-10-573-9, Volume 10, June 2 - 7, 2014, pp. 109-112.

16. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.

17. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната ло-гистика*, Trans&Motauto 2005 с.37-41.

18. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.

19. Kamarashev, G., Dimitrova, S., *Aspects of defence and security resource allocattion*, Sibiu 2007.

20. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 c.30-37.

21. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.