УДК 342.52(043.2)

Яцун О.Д., здобувач вищої освіти
першого (бакалаврського) рівня,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Дей М.О., доктор філософії в галузі права, доцент

КІБЕРЗЛОЧИННІСТЬ В УМОВАХ ПАНДЕМІЇ, ПОВ'ЯЗАНОЇ З COVID-19

Пандемія COVID-19, представляючи гарний ґрунт кіберзлочинної діяльності, дала поштовх для розвитку цієї тенденції, створивши сукупність унікальних обставин, які піддали вразливості як суспільство в цілому, так і кожну організацію. Багатьом довелося адаптуватися, щоб вижити в унікальних суспільних умовах, спричинених пандемією (наприклад, швидкий перехід від фізичного кабінету до віртуального робочого місця в Інтернеті), залишивши персональні дані менш захищеними, ніж раніше.

Досить небезпечним інструментом в руках кіберзлочинців під час пандемії стала соціальна інженерія. Соціальна інженерія – наука про використання соціальної взаємодії як засобу переконати людину чи організацію виконати конкретний запит зловмисника, коли соціальна взаємодія, переконання чи запит стосується сутності, пов'язаної з комп'ютером [1, с. 271]. Тобто, кіберзлочинці впровадили ці технології, щоб скористатися переживаннями та страхами своїх жертв та використати пандемію для шахрайства та нападів.

Як тільки почалася пандемія COVID-19, зловмисники почали реєструвати домени, що містять слова «коронавірус», «covid19» та «корона». Використовуючи ці домени, кіберзлочинці могли видавати себе за державні організації, національні заклади охорони здоров'я або ВООЗ, переконуючи людей робити дії під ілюзією, що вони взаємодіють із законною партією [2]. Також уважно стежачи за світовими тенденціями та новинами, кіберзлочинці скористалися різними урядовими оголошеннями про політику підтримки громадян та економіки для поширення фішингових електронних листів або текстових повідомлень. У цих повідомленнях злочинці мали б ділитися зловмисними зв'язками з особами, які, вводячи свої особисті дані, потім стали жертвами фінансових шахрайств.

Зловмисні веб-сайти також використовувались для встановлення шкідливого програмного забезпечення, яке можна використовувати для отримання даних, порушення роботи служби тощо. Одним із таких прикладів було те, що кіберзлочинці встановили шкідливе програмне забезпечення на основі Java на копію карти, випущеної Університетом

Джона Хопкінса для відстеження поширення вірусу по всьому світу [1, с. 275, 3]. Після завантаження плагіна шкідливе програмне забезпечення отримає віддалений доступ до системи користувача, фотографій пристрою, відео та даних про місцезнаходження.

Також існують програми-вимагателі, найпоширеніші атаки на організації. Зазвичай кіберзлочинці беруть у заручники цінні дані та оперативні активи, щоб збільшити свої шанси отримати виплати/викуп. Лікарні, медичні центри та державні установи були переважною метою цих нападів під час кризи, оскільки вони не могли дозволити собі позбавити своїх даних та систем у таких критичних обставинах і були б готові платити.

Відповідно до розділу 2 Регламенту Європейського парламенту і Ради ЄС 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (або GDPR) [4] підприємства та організації, незалежно від того, є вони приватними чи державними структурами, мають ряд зобов'язань. З одного боку, вони мають застосовувати превентивні організаційні заходи, такі як: реєстри ризиків захисту даних, процедури сповіщення про порушення персональних даних. З іншого боку, технічні заходи, що мають враховувати сучасний рівень техніки. Ці заходи можуть включати двофакторні системи автентифікації, надійну політику щодо паролів та контроль доступу, надійне антивірусне програмне забезпечення та захист кінцевих точок, управління виправленнями та процедури управління уразливістю.

На сьогодні існують дві великі організації, які беруть на себе провідну роль у боротьбі з кіберзлочинністю на міжнародному рівні. Це підрозділ по боротьбі з тероризмом ОБСЄ – організації, що діє під егідою ООН, а також Європол. Також, у Європейському союзі діє Центр по боротьбі з кіберзлочинністю (European CyberCrime Centre).

Крім того, як зазначає Філіп Аманн, керівник стратегії Європейського центру з кіберзлочинності (EC3) Європола: «Кібербезпека є спільною відповідальністю, і, хоча технології можуть забезпечити базовий захист, слід приділити серйозну увагу людським факторам. Це означає, що постійне та цілеспрямоване навчання, освіта та підвищення обізнаності однаково важливі для технологій та доповнюють технологічні заходи для підтримки високого рівня кібербезпеки та стійкості» [5].

Отже, пандемія COVID-19, на тлі багатьох соціальних та економічних проблем, спричинила підвищений рівень кіберзлочинів. Кіберзлочинці особливо швидко пристосувались до ситуації, яка склалась, і почали використовувати методику під назвою соціальна інженерія. У цілому в європейському суспільстві панує думка про те, що поборотися із кіберзлочинністю можна лише у світлі цілісного підходу до захисту даних

та безпеки даних. Тобто, дотримання вимог GDPR, пов'язаних із безпекою, вже передбачало необхідні технічні та організаційні заходи, але лише разом із людським фактором (навчання, освіта співробітників) можна дійти високого рівня кібербезпеки.

Література

1. Mouton F., Leenen L., Malan M.M., Venter H.S. (2014). На шляху до онтологічної моделі, що визначає сферу соціальної інженерії. У: Kimppa K., Whitehouse D., Kuusela T., Phahlamohlaka J. (eds) ICT and Society. HCC 2014. IFIP Advancements in Information and Communication Technology, vol. 431. Springer, Berlin, Heidelberg. С. 266-279.

2. Лаллі С. та ін.: Кібербезпека у вік COVID-19: хронологія та аналіз кіберзлочинів та кібератак під час пандемії. (2020), arXiv, 21 чер. 2020 р. URL: Https://arxiv.org/pdf/2006.11929.pdf

3. Оригінальний ресурсний центр карт та коронавірусу. URL: https://coronavirus.jhu.edu/map.html

4. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27.04.2016 про захист фізичних осіб при обробці персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальне положення про захист даних). URL: http://data.europa.eu/eli/reg/2016/679/oj (дата звернення 28.10.2020).

5. Інтерв'ю з Філіпом Аманом, керівником стратегії Європейського центру з кіберзлочинності (EC3) Європола. URL: https://www.trilateralresearch.com/cyber-threats-and-pandemics-tackling-risk-through-shared-responsibility/