УДК 004.7
Шутко А.С.[1], Зайко Т.А.[2]
[1]студ. гр. КНТ-128 НУ «Запорізька Політехніка»
[2]канд. техн. наук, доц. НУ «Запорізька Політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА-2021. ОСНОВНІ ЗАГРОЗИ, ТРЕНДИ

З упевненістю можна сказати, що Інтернет заволодів усіма аспектами життєдіяльності людини. Існує безліч загроз кібербезпеки, основні з них: DDoS-атаки, шкідливе програмне забезпечення в десктоп і мобільних додатках, уразливості операційних систем, фішингові атаки, парольні атаки, атаки на пристрої Інтернету речей, витоки даних та ін. Пандемія COVID-19 привела до суттєвого зростання кіберзлочинності, примусивши співробітників працювати з дому, де вони більш уразливі. З'явилися нові загрози, нові методи і засоби захисту і, звичайно ж, серйозно змінилися тренди в розвитку галузі.

До актуальних загроз в інформаційній безпеці 2021 року можна віднести: атаки підприємств через віддалених співробітників, витік даних, атаки на 5G-мережі та атаки з використанням штучного інтелекту. Відбувається зростання діяльності шифрувальників та фішингу.

Ще до пандемії багато компаній переходили на віддалену роботу. Немає сумнівів в тому, що дистанційна робота має ряд переваг як для співробітників, так і для їх організацій, але це також проблема для кібербезпеки. Самий поширений варіант атаки – коли зловмисники отримують доступ до службового облікового запису жертви. Тепер це простіше, тому що віддалені співробітники залишилися без нагляду фахівців з інформаційної безпеки; деякі компанії досі не оновили політику безпеки; до того ж працівники часто підключаються до корпоративної мережі з особистих пристроїв. На цьому тлі прийоми соціальної інженерії і теж вірусне ПЗ працюють ефективніше, ніж будь-коли.

Говорячи про витік даних, важливо зауважити, що зловмисники отримують доступ до корпоративних мереж найчастіше шляхом крадіжки облікових даних співробітників. Бо вони використовують пристрої, що не оновлюються, не керуються і не захищені корпоративним IT-відділом.

5G – благодатне середовище для кіберзлочинців. Прогалини в захисті доведеться усувати по ходу справи, і на те, щоб забезпечити прийнятний рівень безпеки технології, піде, певно, не один рік. Стек технологій в 5G потенційно залишає злочинцям можливість здійснювати атаки на абонентів і мережу оператора. Такі атаки можуть бути виконані з мережі міжнародного роумінгу, мережі оператора або партнерських мереж, які надають доступ до послуг.

Крім цього, штучний інтелект тепер теж на озброєнні кіберзлочинців. Зловмисники все активніше використовують можливості ШІ і машинного навчання. Просунуті кіберзлочинці застосовують ШІ, щоб складати профіль жертв і знаходити уразливості в застарілих інформаційних системах. Також все більше з'являється доступних фреймворків ШІ, які можна використовувати за передплатою, тобто розробляти ефективні інструменти для атак без серйозних вкладень.

Майже третина атак була пов'язана з методами соціальної інженерії, де кіберзлочинці намагаються використовувати страх, пов'язаний з пандемією COVID-19, як частину своєї тактики. На жаль, фішингові та спуфінгові атаки, пов'язані з пандемією, стали серйозною проблемою в 2021 році. Атаки часто збігаються з великими подіями, такими як спалах нових випадків або оголошення про нові ліки або вакцини. Їх мета – змусити нічого непідозрюючих жертв натиснути шкідливе посилання, щоб передати конфіденційну інформацію.

Не менш важливим фактом є те, що в цьому році зросла кількість атак шифрувальників – шкідливого ПЗ, яке шифрує дані, блокує роботу і нерідко вимагає викуп. Також популярність здобув шантаж викраденими приватними даними. Це перетворилося на повноцінну індустрію: зловмисники навіть створили власні сайти і аукціони для продажу викраденої інформації. Таким чином загальна сума вимог про викуп в 2020 році досягла 1,4 мільярда доларів, а середня сума відшкодування збитку – 1,45 мільйона доларів. Вимагачі є третім за популярністю типом шкідливих програм, що використовуються при витоку даних.

Крім вищенаведених загроз інформаційної безпеки, зросли DDoS-атаки. DDoS-атака містить в собі перевантаження сервера великими обсягами трафіку, щоб вивести з ладу бізнес-сайт. Такі напади останнім часом стали досить частими. Наприклад, у 2020 році було зроблено 4,83 мільйони DDoS-атак та порушення роботи сервісу може коштувати бізнесу в середньому до 100 тисяч доларів кожної години.

Поки триває пандемія, ринок хмарних обчислень збільшився на 50%. Хоча хмарна інфраструктура дуже безпечна, клієнти несуть відповідальність за реалізацію функцій кібербезпеки та їх правильне налаштування. Неправильна конфігурація хмари – поширене джерело витоку даних, яке зростає в міру того, як все більше компаній впроваджують хмарні сервіси для підтримки віддалених співробітників. Таким чином було здійснено 7,5 мільйона атак на хмарні акаунти в 2021 році. З початку року кількість спроб зросла на 250% в порівнянні з 2020 роком.

Підводячи підсумки можна сказати, що пандемія COVID-19 вплинула на зростання кіберзлочинності і на весь IT-світ. Компанії почали працювати віддалено і працювати з хмарними платформами. Витонченість загроз зросла

через застосування нових технологій, таких як машинне навчання, штучний інтелект і впровадженого 5G. Все це говорить про те, що індустрія кібербезпеки як ніколи важлива.