УДК 004.49+005
Віталій Кравчук, магістр спеціальності 125 - Кібербезпека
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМА ЗАХИСТУ КІБЕРПРОСТОРУ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Vitaliy Kravchuk, master's degree in 125 – Cybersecurity

CYBERSECURITY ISSUES FOR SMALL AND MEDIUM-SIZED BUSINESSES

У сучасних реаліях важко уявити побудову успішної бізнес-моделі без кіберпростору. Компанії дедалі більше переходять на віддалену роботу, це призводить до розвитку IT-інфраструктури і водночас збільшення кількості кібератак на дану галузь.

Багато власників компаній малого і середнього бізнесу не розуміють потреби у витратах на захист компанії від кіберзагроз. Однак така ситуація триває доти, доки власник не зіткнеться з кібератакою, яка може призвести до блокування процесів і сервісів підприємства, фінансових втрат, а в гіршому випадку до повної зупинки чи втрати бізнесу [3].

Щороку експерти Міжнародної спілки електрозв'язку ООН (International Telecommunication Union) складають рейтинг країн за рівнем кібербезпеки під назвою «Глобальний індекс кібербезпеки» (Global Cybersecurity Index). У відповідній доповіді фахівці ITU оцінюють комп'ютерну безпеку всіх країн світу за п'ятьма параметрами: юридична, технічна, організаційна підготовленість, готовність до співпраці, розвиток освітнього та дослідницького потенціалу країни. Найбільш актуальна версія дослідження була випущена у 2020 році. За кількістю кібератак Україна знаходиться на 86-у місці у світі [1].

З вище написаного ми можемо зробити висновок, що найчастіше проблеми та загрози зустрічаються у малому та середньому бізнесі. Серед них:

Незахищеність периметру. Неналаштований мережевий захист, неналаштований захист серверів і кінцевих пристроїв, відсутність систем моніторингу та системи резервного копіювання рано чи пізно призводить до злому IT-інфраструктури.

Незахищеність інформації та баз даних. Бухгалтерська інформація, фінансова інформація, звіти до контролюючих органів, база даних клієнтів, листування з важливими клієнтами або партнерами, особиста конфіденційна інформація тощо.

Незахищеність каналів передачі. Більшість компаній нині потребує доступу до своєї IT-інфраструктури 24/7 з будь-якої точки світу. Для ефективної роботи необхідний швидкий, безпечний канал передачі інформації. Це розуміють керівники, а також зловмисники, тому часто замість атаки на IT-інфраструктуру вибирають атаку на канали передачі інформації.

Неналежний антивірусний захист. Комп'ютерний вірус - вид шкідливих програм, здатних впроваджуватися в код інших програм, системні області пам'яті, завантажувальні сектори та розповсюджувати свої копії різноманітними каналами зв'язку.

Основна мета вірусу – його поширення. Крім того, часто його супутньою функцією є порушення роботи програмно-апаратних комплексів — видалення файлів, видалення операційної системи, непридатність структур розміщення даних, порушення працездатності мережевих структур, крадіжка особистих даних, вимагання, блокування роботи користувачів тощо [4].

Щодня з'являються нові комп'ютерні віруси, виконують певні завдання: від простих – збирання інформації, до складніших процесів – шифрування інформації або використання шкідливих дій.

Неналежний захист сайту. Говорять, якщо вас немає в інтернеті, вас немає у бізнесі. Сайт – це обличчя і вітрина компанії, нікому не хочеться втратити обличчя.

Неналежний захист програм і додатків. Пошта, месенджери, інші програми, які використовують для роботи та спілкування з клієнтами. Якщо програми і канали спілкування зламають, отримають з них конфіденційні дані та почнуть розсилати через них шкідливу інформацію, це може призвести до втрати репутації, коштів, а іноді й клієнтів.

У результаті всіх вищезазначених загроз є ризик втрати дуже важливих даних (sensitive data). Sensitive data - дуже важливі дані, такі як: персональні дані користувачів; банківські та медичні дані; паролі; інформація про фінансові операції тощо. [2] Саме за ними, як правило, полюють хакери, прогнози їх втрат досить великі.

Аби запобігти втраті даних треба ідентифікувати ризики і загрози та почати працювати над запровадженням кіберзахисту компанії. Ідентифікація ризиків і загроз починається з аналізу вразливості підприємства. Параметри аналізу формуються під кожну компанію індивідуально, як правило, проходять у таких напрямках: аудит інформаційних потоків, аудит баз і середовища зберігання, права доступу до інформації, кіберзагроз, мережі, серверів, програм, сервісів, додатків і робочих місць кінцевих користувачів. За результатами перевірки формується звіт, на основі якого будується проект захищеної IT-інфраструктури [5].

Таким чином, безпечне функціонування бізнесу залежить від системи захисту даних, яка впроваджена на підприємстві. Щорічна статистика показує, що кількість кібератак у світі зростає, від чого несе збитки бізнес-сектор. Якщо компанія прагне стійко зростати, треба визначити потенційні ризики та загрози і почати розробку заходів для підвищення кібербезпеки.

Література

1. https://nonews.co/directory/lists/countries/cybersecurity-index
2. https://www.dataprivacyframework.gov/s/article/1-Sensitive-Data-dpf
3. Pescatore J. SANS 2021 Top New Attacks and Threat Report [Електронний ресурс] / John Pescatore. – 2021. – Режим доступу до ресурсу: https://fs.hubspotusercontent00.net/hubfs/8645105/white-paper/sans-attack-threatreport-2021.pdf.
4. Дубов, Дмитро Володимирович. "Стратегічні аспекти кібербезпеки України." Стратегічні пріоритети 4 (2013): 29.
5. Гриник, Р. О. Дослідження проблем захисту сучасного кіберпростору України / Р. О. Гриник, М. В. Маржан // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 30–31.