УДК 004.056.5

О. В. Кареліна к. пед. н., доц.
Тернопільський національний технічний університет ім. І. Пулюя, Україна

ЛАНДШАФТ КІБЕРЗАГРОЗ ДЛЯ БІЗНЕСУ

O. V. Karelina Ph. D. Assoc., Prof.
Ternopil Ivan Puluj National Technical University, Ukraine

LANDSCAPE OF CYBER THREATS TO BUSINESS

У 2020 р. онлайн-діяльність всіх компаній значно активізувалась, з'явився цифровий формат у тих підприємств, які раніше його не мали. Діджиталізація надає можливість працювати у реаліях сучасних загроз. Однак така ж зростаюча активність характерна і для середовища кіберзловмисників, які атакують і великі корпорації і платежі фізичних осіб.

За даними Всесвітнього економічного форуму [1], кібератаки є глобальною проблемою №2 у країнах з розвиненою економікою, поступаючись за небезпечністю лише фінансовій кризі. Багато відомих компаній у 2020 р. стали жертвами ransomware – хакерських програм, які шифрують дані і вимагають викуп за відновлення роботи. Хакери сприймають таку діяльність як свій бізнес та сформували поняття Ransomware-As-A-Service, поширюючи свої технології на умовах франчайзингу. Хакери пропонують і послуги із захисту інформації від інших зловмисників, наприклад, угруповання CLOP оцінює таку послугу у $250 000. Кількість атак з вимогою викупу зросла на 45% порівняно з 2019 р. [2]. Жертвами стали компанії різних галузей: виробники автомобілів Honda та Mercedes-Benz Superdome, один із найбільших європейських розробників програмного забезпечення SoftwareAG, розробники ігор Crytec та Ubisoft, продавець книг Barnes & Noble Booksellers, Inc., виробник медичної техніки OHST Medizintechnik AG, виробник металу Stromberg Metal Works, Inc., виробник промислових роботів Yaskawa Electric Corporation та багато інших. Викуп за розблокування корпоративної інформації встановлюється у кількадесят тисяч доларів, зловмисники можуть вимагати й сотні тисяч доларів та навіть мільйони залежно від обсягу прибутків компанії.

Є кілька векторів проникнення шкідливого програмного забезпечення: електронна пошта, браузер, пристрої інтернету речей, RDP та SSH з'єднання, активи компанії у хмарах тощо. Поширення фішингових листів – один із найпростіших варіантів надіслати шкідливе програмне забезпечення, але він спрацьовує вже багато років. У 2020 р. шкідливі програми найчастіше інтегрували у файли .pdf, прикріплені до фішингового листа (54% зловмисних додатків до листів). 17% шкідливих файлів інтегрували в .html. 6% листів містили .xls-вкладення, 5% - JavaScript-файли інтегровані в документи MS Word [2].

Найпопулярніший у хакерів метод зараження комп'ютера у перші місяці 2020 р. – атака на браузер [3]. Причина такого вектору атаки – значне зростання кількості працівників, які виконують роботу з віддалених робочих місць. Шкідливе програмне забезпечення завантажується з фішингового сайту. Пандемія кардинально змінила поняття периметру організації, який захищає департамент кібербезпеки. Тепер до нього належать віддалені робочі місця, організовані вдома у працівників на базі їх власних технічних засобів.

Технічні засоби теж є цілями для атак. Крім вразливостей комп'ютерної техніки хакери активно експлуатують для проникнення у мережу і вразливості інтернету речей (роутерів, принтерів, відеокамер тощо). Будь-який пристрій, керований програмним забезпеченням та підключений до інтернет може бути атакований і використаний зловмисниками. 35% власників розумних гаджетів недооцінюють небезпеку і не змінюють заводський логін і пароль керування пристроєм [4]. Заводські установки доступні, наприклад, на сайті https://passwordsdatabase.com/ і будь-хто може авторизуватись.

Сучасні системи SCADA управління виробництвом, нафтодобуванням, водо- та електропостачанням теж комп'ютеризовані та вразливі до атак. У червні виповнилось 10 років вірусу Stuxnet – найвідомішому атакувальнику виробничих систем, який вивів з ладу

обладнання на іранській ядерній станції збагачення урану. Саме Stuxnet став кіберзброєю, яка вразила ціль, спричинивши навіть більші руйнування, ніж військова зброя.

То як захистити бізнес у сучасних реаліях кіберзагроз? Для будь-якої компанії на сьогодні необхідним є департамент кібербезпеки, так само як бухгалтерія, відділ кадрів, інші підрозділи, які забезпечують основну діяльність. Збудувати належний рівень захисту може бути надто затратно, зважаючи на вартість обладнання, програмного забезпечення, розмір зарплати фахівців. Та й знайти фахівців на сучасному ринку праці ІТ вдасться не завжди. Глобальний дефіцит працівників інформаційної безпеки становить 4 мільйони [5].

Захист інформації можна придбати як послугу у спеціалізованих компаній з кібербезпеки. Універсальними методами захисту від автоматичних та спрямованих атак є встановлення антивірусів, веб-фільтрів, антиспам-систем, сканування внутрішнього та зовнішнього периметра на вразливості, оновлення програмного забезпечення. Компанії з кібербезпеки розробляють власні унікальні методики протидії загрозам, які базуються на штучному інтелекті, аналізують дані в даркнеті (анонімізованій мережі, де й зосереджується активність хакерів та інших порушників закону).

Атаки здійснюються на бізнеси усіх галузей, не уникнути їх як гігантам виробництва, так і дрібним компаніям. Втрати від атаки можуть бути важкими або й непоправними, коли підприємство припиняє своє функціонування. Найбільш вдалий момент для захисту інформації – сьогодні. Завдяки світовій спільноті фахівців з інформаційної безпеки розроблені методи боротьби з найнебезпечнішими впливами і ведеться безперервний моніторинг кіберсередовища для виявлення і нейтралізації нових загроз.

Література:

1. Smith-Bingham R. This is what CEOs around the world see as the biggest risks to business. URL: https://www.weforum.org/agenda/2019/10/risks-to-doing-business-2019-developing-developed/ Last accessed 30.10.20
2. Как пандемия меняет ландшафт киберугроз. Блог компании Trend Micro. URL: https://habr.com/ru/company/trendmicro/blog/525502/ Дата доступа 30.10.20
3. FortiGuard Labs: пандемия кардинально повлияла на ландшафт киберугроз. URL: https://www.pcweek.ua/themes/detail.php?ID=161621 Дата доступа 31.10.20
4. Чем опасны хакерские атаки на IoT-устройства: реальные истории. URL: https://habr.com/ru/company/kauri_iot/blog/473532/ Дата доступа 31.10.20
5. Костылева Т. Дефицит кадров в области кибербезопасности превысил 4 миллиона специалистов. URL: https://d-russia.ru/defitsit-kadrov-v-oblasti-kiberbezopasnosti-prevysil-4-milliona-spetsialistov.html Дата доступа 31.10.20