УДК 338

Федишин І.Б.
Тернопільський національний технічний університет ім. Івана Пулюя

НОВІТНІ ВИКЛИКИ ТА ЗАГРОЗИ ДЛЯ НАУКИ ТА БІЗНЕСУ. КІБЕРАТАКИ

Fedyshyn I.

NEW CHALLENGES AND THREATS FOR SCIENCE AND BUSINESS. CYBERATTACKS

Інтернет розроблявся з метою забезпечення взаємодії віддалених комп'ютерів і задумувався як децентралізована територіально розподілена мережа з безліччю альтернативних пунктів збереження і шляхів поширення інформації. Передбачалося, що це дозволить забезпечити надійну взаємодію комп'ютерів Міністерства оборони США, навіть у випадку, якщо частина мережі вийде з ладу унаслідок воєнних дій, наприклад, ядерних вибухів.

Реальний кіберпростір складається з фізичної інфраструктури, яка функціонує завдяки підтримці інформаційної інфраструктури. Крім таких пристроїв, як смартфони або комп'ютери, фізичними компонентами мережі Інтернет також можна вважати сервери та центри обробки даних (де зберігаються і обробляються дані, доступні в мережі), точки обміну Інтернет-трафіком (інфраструктура, що упорядкує обмін даними), центри управління мережею (здійснюють моніторинг та управління веб-трафіком), а також волоконно-оптичні кабелі, які уможливлюють фізичне з'єднання між користувачами в різних країнах по всьому світові.

Невпинне зростання користувачів Internet в останні роки спричинило появу в мережі багатьох негативних явищ. Покупки товарів з чужими кредитними картками, крадіжки інтелектуальної власності в Internet набули величезного розмаху. Основною проблемою безпеки кіберпростору з часу його виникнення була проблема передавання закритої інформації через відкриту мережу.

Кіберзагрози притаманні не лише великим підприємствам, але й суб'єктам малого та середнього бізнесу (МСБ). Інколи останні стикаються з цим явищем набагато частіше, оскільки МСБ, як правило, є більш уразливі з меншою кількістю заходів безпеки.

Загроза кібератак зростає у все більш оцифрованому світі. Навіть для компаній, які впровадили провідні цифрові технології та кібербезпеку до COVID-19, перехід на віддалену роботу створює додаткові ризики.

Дослідження Check Point Research (CPR) виявило, що глобальні атаки зросли на 28% у третьому кварталі 2022 року порівняно з тим самим періодом 2021 року. Середня тижнева кількість атак на організацію в усьому світі досягла понад 1130 у 2022 році.

У звіті, опублікованому в серпні 2022 року, CPR зазначив, що сектор освіти зазнавав більше ніж подвійних атак на тиждень порівняно з іншими галузями. Ця тенденція продовжувалася: у третьому кварталі 2022 року - освітній/дослідницький сектор щотижня стикався з 2148 атаками на організацію, що на 18% більше, ніж у третьому кварталі попереднього року.

Наукові заклади стали популярною мішенню для кіберзлочинців після швидкої оцифровки, яку вони розпочали у відповідь на пандемію COVID-19. Багато з них були погано підготовлені до несподіваного переходу до онлайн-навчання, що створило широкі можливості для хакерів проникнути в мережі будь-якими засобами. Школи та університети також стикаються з унікальною проблемою роботи з дітьми чи молодими людьми, багато з яких використовують власні пристрої, працюють у публічних місцях і часто підключаються до загальнодоступного Wi-Fi, не думаючи про наслідки і безпеки для пристрою і передачі даних.

Другою найбільш постраждалою від кібератак галуззю стала державна/військова сфера з 1564 щотижневими атаками у 2022 році, що на 20% більше, ніж за той самий період 2021 року. У секторі охорони здоров'я відбулися найбільші зміни порівняно з 2021 роком, у середньому там відбувалося 1426 атак на тиждень –збільшення на 60% у 2022 році в порівнянні із 2021 роком.

Лише через три дні після вторгнення в Україну, 27 лютого 2022 р., Check Point Research (CPR) відзначив зростання кількості кібератак на урядовий і військовий сектор України на 196%.

Середньостистичну щотижневу кількість кібератак на підприємство в залежності від галузі у третьому кварталі 2022 року подано на рисунку 1.

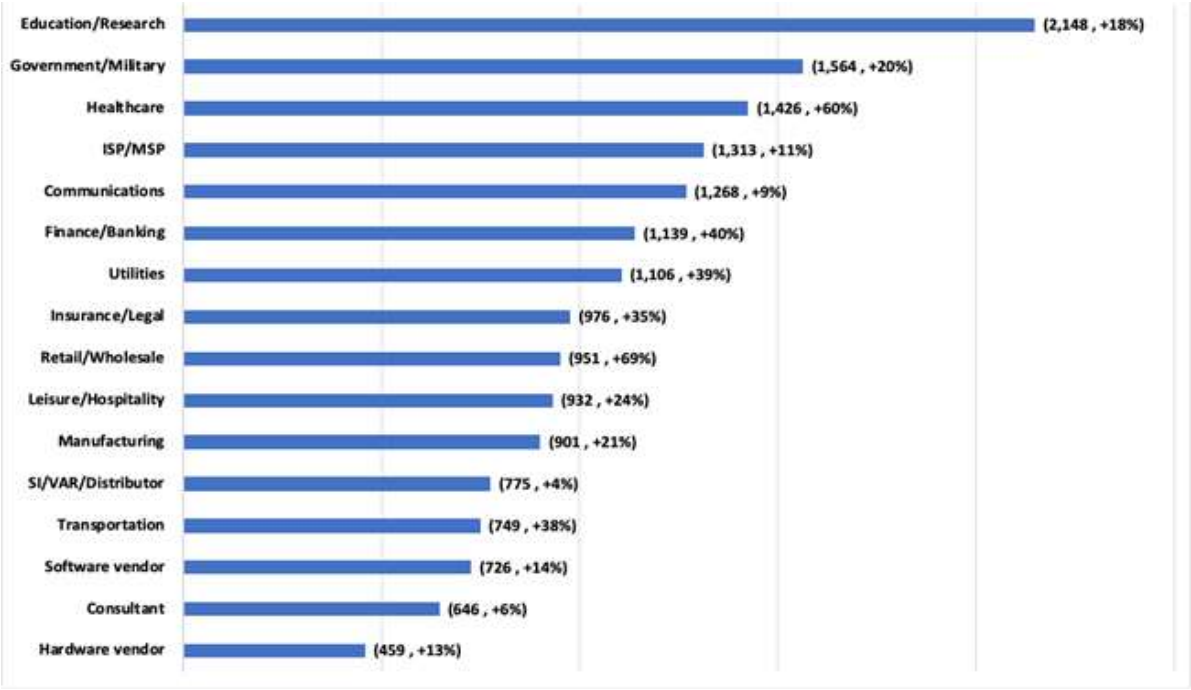

Рис.1 Середньостистична щотижнева кількість кібератак на підприємство в залежності від галузі у третьому кварталі 2022 року

З метою ефективного протистояння негативним впливам на кіберпростір необхідно розробити інструмент для систематичного вивчення потенційних загроз, які можуть спровокувати появу нового ризику або зміни характеру вже ідентифікованого ризику, щоб потенційні та нові загрози могли бути визначені, оцінені і пом'якшені якомога раніше.

Список використаних джерел:

1. Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed. URL: https://pages.checkpoint.com/cyber-security-report-2022.html

2. World Travel & Tourism Council: To Recovery & Beyond: The Future of Travel & Tourism in the Wake of COVID-19 - 2020. URL: https://wttc.org/Portals/0/Documents/Reports/2020/To%20Recovery%20and%20Beyond-The%20Future%20of%20Travel%20Tourism%20in%20the%20Wake%20of%20COVID-19.pdf?ver=2021-02-25-183120-543