НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

**ЦЕНТР БЕЗПЕКОВИХ ДОСЛІДЖЕНЬ**
*CENTER FOR SECURITY STUDIES*

# ДОСЛІДЖЕННЯ ЩОДО БЕЗПЕКИ ДАНИХ ВІД VERIZON: ГОЛОВНІ ВИСНОВКИ

**С. Гнатюк,** *канд. іст. наук, головний консультант відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень*

Звіт «*The 2021 Data Breach Investigations Report*»[1], який підготували фахівці одного з провідних світових вендорів *Verizon*, містить відомості та висновки щодо широкого спектра показників і тенденцій, пов'язаних з інцидентами порушення безпеки даних упродовж 2021 р. Автори наголошують, що звіт не є спробою «передбачити майбутнє», проте завдяки застосованим у ньому методологіям, дає змогу організаціям розрахувати сценарії та обрати адекватну їх можливостям стратегію реагування (*response*) «перед обличчям невизначеного майбутнього».

Дослідження базовано на корпусі даних з різноманітних джерел, зокрема з прикладами, наданими Консультативним центром досліджень загроз *Verizon* (*Verizon Threat Research Advisory Center*), зовнішніми партнерськими звітами, а також опублікованими відомостями про безпекові інциденти. Результати аналізу – майже 30000 загроз, 5258 підтверджених порушень і 14 мільйонів розслідувань – викладено в доступній візуалізованій формі.

Вивчивши ці дані, фахівці *Verizon* дійшли низки висновків, ключовими з яких є такі.

- Загалом ***85 % розглянутих у звіті порушень так чи інакше пов'язані з людським фактором***.
- Фішинг (*phishing*) у 2021 р., як і раніше, був найпопулярнішою тактикою порушення безпеки даних. ***Порівняно з попереднім 2020 р. кількість інцидентів із застосуванням фішингу зросла ще на 11 % та досягла 36 % їх загальної кількості.*** Велику роль відіграло поширення COVID-19, що спричинило збільшення комунікацій та замовлень онлайн і дало зловмисникам нову тему для маніпуляцій.
- Друге місце посіла компрометація корпоративних імейлів (*Business Email Compromises – BECs*). ***2021 р. кількість випадків уведення в оману (misrepresentation) користувачів виявилася в 15 разів більшою проти попереднього року.***
- ***Удвічі частіше (у 10 % випадків), як порівняти з 2020 р., застосували програми-вимагачі (ransomware),*** що 2021 р. опинилися на третьому місці. Таке зростання зумовлено новими зловмисними тактиками, як-от викрадення даних під час їх шифрування.
- ***Основним вектором хакерських атак досі є вебдодатки***, причому ***80 % таких атак спричиняють порушення безпеки даних.*** Так, на друге місце в *Hacking*

[1] Див.: URL: https://www.verizon.com/business/resources/reports/dbir/

*vectors* перемістилися програми шерингу робочого столу ПК (*screensharing, desktop sharing*).

- Інциденти й порушення безпеки даних 2021 р. ***внаслідок компрометації активів організацій відбувалися в зовнішніх хмарних сховищах*** (*external cloud assets*) ***частіше***, аніж на домашніх серверах у приміщеннях (*on-premises assets*). Отже, кількість скомпрометованих персональних пристроїв знизилася.
- ***61 % порушень безпеки даних були пов'язані з обліковими даними.***
- Медіанне значення втрат від інцидентів 2021 р. склало $ 21659 при загальному діапазоні сум таких утрат від $ 826 до $ 653587.

У документі окреслено також низку трендів, що з'явилися 2021 р.

Пріоритетними векторами порушень стають соціальні сервіси та вебдодатки, використання вкрадених облікових даних для компрометації сервісів електронної пошти на хмарних платформах (*cloud-based email systems*).

Попри численні прогнози щодо сплеску фішингу, здирництва, крадіжки / використання облікових даних унаслідок пандемії COVID-19, її реальний вплив виявися не надто значним (наприклад, показники фішингу зросли на 11 %).

Сталими є дві тенденції: пріоритетним об'єктом для шахраїв так само є облікові та персональні (з-поміж них банківські) дані, а їхня головна мотивація найчастіше – фінансовий прибуток.