◆ ДЕМОНСТРАЦІЙНИЙ ЗРАЗОК · ДАНІ ЗНЕОСОБЛЕНІ

ЗВІТ · ЗАХИСТ РЕПУТАЦІЇ (REPUTATION DEFENSE) · БАЗОВИЙ АУДИТ

Подивіться на себе очима того, хто готує проти вас атаку.

Власник замовив базовий аудит перед раундом переговорів і публічним виходом компанії. Він був певен, що ззовні все закрито. За п'ять днів ми зайшли на бренд «X» так, як зайшов би зловмисник, і знайшли дві відкриті двері, про які в компанії ніхто не знав: робочі паролі співробітників у старих витоках і фейковий домен-двійник, майже не відрізнити від справжнього, уже зареєстрований на сторонню особу.

РІВЕНЬ ПОСЛУГИ	ВАРТІСТЬ
Базовий аудит (Red Team на вас)	**$399 разово**
СТРОК ВИКОНАННЯ	РІВЕНЬ ВРАЗЛИВОСТІ
5–7 днів	**44 / 100 — є відкриті двері**
ДЖЕРЕЛА	ВЕРДИКТ
Публічна поверхня + витоки	**2 вектори потребують закриття**

Головне одним рядком. Ваш бренд не зламаний і не в кризі. Але зловмисник уже мав би дві готові точки входу: облікові дані з витоків і домен-двійник під фішинг ваших клієнтів. Це відчинені двері, а не пожежа. Їх закривають за кілька днів, поки ними ще ніхто не скористався.

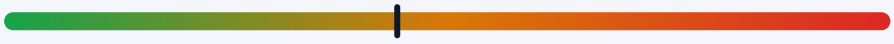
1 Рівень вразливості

44/100

ІНДЕКС ВІДКРИТОСТІ

Є відкриті двері

Індекс відкритості показує, наскільки легко зайти на вас ззовні. Чим вище бал, тим більше готових точок входу для атакувальника. 44 — помірна експозиція: критичного компромату немає й публічна репутація чиста, але два вектори дають зловмиснику реальну двері всередину. Мета аудиту — закрити їх, поки індекс не почав працювати проти вас.



0 — закрито 50 100 — відкрито настіж

2 Вектори атаки

ВЕКТОР АТАКИ	СТАН	ЩО ЦЕ ДАЄ ЗЛОВМИСНИКУ
Витоки корп-даних у breach-базах	Ризик	Робочі логіни й паролі співробітників у старих зливах; частина ще діюча
Impersonation — домени й акаунти під бренд	Ризик	Зареєстровано домен-двійник із поштовими записами; готова інфраструктура під фішинг клієнтів і партнерів
Наявний компромат чи негатив	Увага	Один старий конфлікт у пошуковій видачі; зараз тихий, але легко піднімається
Відкрита поверхня — сліди й люди	Увага	Робочі email у відкритому доступі, видно ключових людей і структуру — матеріал під соц-інженерію

Два **червоні** вектори (витоки й домен-двійник) — це те, чим зловмисник скористався б першим, і саме вони тягнуть індекс угору. Жовті не термінові, але їх варто прибрати, поки вони не стали важелем у чужих руках.

3 Що знайдено по кожному вектору

Витоки корп-даних (червоний)

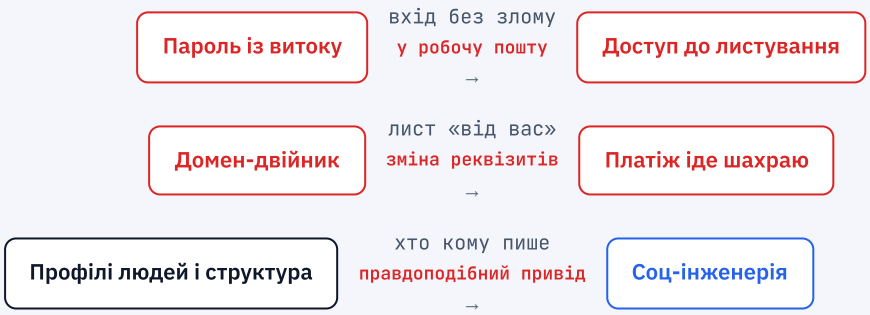
У відкритих breach-базах знайдено кілька корпоративних адрес @бренд-X із паролями зі старих зливів. Дві пари логін-пароль збігаються з форматом, який компанія використовує досі, тож найімовірніше ще робочі. Через них зловмисник заходить у пошту без жодного «злому»: просто вводить те, що вже лежить у відкритому доступі.

Impersonation — домен-двійник (червоний)

Зареєстровано домен, що відрізняється від вашого однією літерою. На ньому вже стоять поштові записи, тобто з нього можна слати листи «від вашого імені». Поки домен активний, будь-хто пише вашому клієнту від імені компанії й просить змінити реквізити оплати.

Жовті вектори. Старий негатив у видачі й відкриті робочі контакти самі по собі не є атакою. Але для того, хто готує соц-інженерію, це матеріал: знаючи людей і структуру, легше скласти переконливий лист під пароль вище.

4 Хто і як міг би це використати



Реальний сценарій: зловмисник бере пароль із витоку, заходить у пошту співробітника, вивчає листування, а тоді з домену-двійника пише клієнту прохання оплатити на «оновлені» реквізити. Жодного зламу, усе зібрано з відкритого. Про це ви дізнаєтесь останнім.

5 Доказова база

Кожна знахідка спирається на зафіксоване джерело: коли знайдено, де саме, збережена копія та її контрольна сума. Двері, які ми показали, — це доказ для вашої команди чи юриста, а не переказ.

ДАТА	ДЖЕРЕЛО	КОПІЯ	ХЕШ
Момент фіксації в UTC	Точна адреса бази / сторінки	Збережений витяг / скрін	SHA-256 копії — незмінність

6 Що робити в перші кроки

Порядок за пріоритетом: спершу закриваємо два червоні вектори, тоді прибираємо матеріал під соц-інженерію.

1 Скинути паролі й увімкнути двофакторку

Поміняйте паролі на всіх адресах із витоків і ввімкніть двофакторку. Це закриває найдешевший вхід уже за день.

2 Забрати або заблокувати домен-двійник

Скарга реєстратору й у сервіси захисту бренду, доказова фіксація домену. Поки він живий, вашим ім'ям обманюють ваших клієнтів.

3 Попередити команду й ключових клієнтів

Одне коротке попередження: можливі листи з підробленого домену, реквізити оплати міняємо тільки з підтвердженням по телефону.

4 Прибрати зайві сліди з відкритої поверхні

Приберіть службові адреси зі старих публікацій, обмежте видиму структуру. Менше матеріалу — складніша соц-інженерія.

7 Звідки дані

- Публічні breach-бази витоків (email, паролі)
- Реєстри доменів і DNS-записи
- Відкриті профілі й соцмережі співробітників
- Медіа та пошукова видача
- Санкційні та «зливні» списки

Конкретні платні сервіси навмисно не називаємо — це наша робоча кухня. Для вас важливий результат і те, що кожне джерело відкрите й зафіксоване.

8 Межі та застереження

Це демонстраційний зразок. Дані знеособлені й не стосуються конкретної компанії. Формат, логіка і глибина справжні; так виглядає реальний базовий аудит після узгодження обсягу.

Працюємо тільки з публічною поверхнею. Ми не зламуємо, не імперсонуємо й не платимо за «пробив». Дивимось лише на те, що вже відкрито назовні, і показуємо це вам першими.

Це не юридична консультація. Argus дає карту вразливостей і план дій. Рішення про юридичні кроки (скарги, блокування домену, звернення до поліції) лишаються за вами та вашими юристами.