ПОСЛУГА ВІД БДО В УКРАЇНІ З КІБЕРЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

Дані авторитетних джерел стверджують, що загальна кількість кіберзлочинів внаслідок пандемії COVID-19 збільшилась у неймовірні ×7 разів! Нажаль Україна – частина цієї жахливої статистики, адже тільки в нашій країні через приблизно 2,7 млн. відкритих портів (вразливі мережеві вузли) можуть бути атаковані будь-які корпоративні мережі. А майже 3 тис. баз даних із персональними даними вже знаходяться у відкритому доступі й можуть бути використані ким завгодно.

Водночас за останній рік побільшало невтішних новин про лихі кібератаки зловмисників, що спочатку шифрують деякі елементи інфраструктури (напр. маршрутизатори), а згодом шантажують бізнес викупом в криптовалютах. Вже достатня кількість відомих українських компаній в тією чи іншою мірою мали вкрай негативний досвід таких інцидентів і далеко не завжди шахраїв було покарано, у той час як бізнес несе колосальні фінансові та репутаційні втрати.

В тому випадку, якщо:

- Останнім часом ваша компанія активно розбудовувала власну систему кібербезпеки
- Бізнес готується до активного росту через канали e-commerce
- Компанія має добре відомий, авторитетний бренд і публічних власників
- У своїй комерційній діяльності ви опрацьовуєте велику кількість персональних даних фізичних осіб
- Галузеві практики чи державний нагляд потребують виконання стандартів з кібербезпеки і/або комплаєнсу щодо цифрових активів

наймовірніше, ваша корпоративна мережа дуже приваблива для хакерських атак,а отже – потребує тестування на стійкість цілеспрямованим загрозам.

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

ЩО ЦЕ?

Метод оцінки готовності IT-інфраструктури компанії до захисту від зовнішніх загроз, що повністю імітує потенційну атаку кібер-злочинців. Команда IT-фахівців входить у роль хакерів і намагається зламати систему за попереднім погодженням з власниками корпоративної мережі, використовуючи всі можливі вразливості системи.

BDO DIGITAL

ПОСЛУГА ВІД БДО В УКРАЇНІ З КІБЕРЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

ЯК ПРАЦЮЄ?

Нашими фахівцями буде проведено спробу на проникнення до внутрішньої мережі компанії у форматі імітації атаки зловмисниками. Під час цього етичного інтрузивного тесту буде досліджено:

- дієвість захисту внутрішньої інфраструктури
- вразливість WI-FI обладнання
- аналіз ризиків загублених/викрадених мобільних пристроїв *(імітація з будь-яким ноутбуком замовника)**
- ефективність використання кібер-вразливостей, що були знайдені під час атаки

** Ексклюзивна пропозиція від BDO в Україні*

НАВІЩО ПОТРІБНО?

Щоб протестувати готовність наявної системи кібербезпеки компанії в реальних умовах

Відпрацювати на практиці сценарії розвитку подій при спробах зовнішніх атак

ЩО В РЕЗУЛЬТАТІ?

1 Детальний технічний звіт щодо виявлених кібер-вразливостей та лаконічний огляд для вищого керівництва

Стандарти, що використовуються:
PTEST, NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OSSTMM, BSI, SANS TOP 25

Стандарти звіту:
Common Vulnerabilities and Exposures (CVE) Compatible, Common Weakness Enumeration (CWE) Compatible, Common Vulnerability Scoring System (CVSSv3.1)

2 За результатами усунення вразливостей проведення повторного тестування на проникнення (входить до пропозиції)

Зацікавилися?

Контакти для звернення:

АНДРІЙ БОРЕНКОВ
Директор "БДО Консалтинг"

aborenkov@bdo.ua
+380 50 380 96 01

BDO in Ukraine
www.bdo.ua
info@bdo.ua

BDO DIGITAL