INTRODUCTION TO CYBERSECURITY

Made by Roman Vasylyshyn

Огляд комп'ютерної безпеки

- Популярність кібер-злочину збільшується – фінансові втрати 2015 року становили $3T, проекція втрат до 2025 року - $10.5T
- Збільшує попит на комп'ютерну безпеку – збільшення витрат на нових фахівців та навчання безпеки у компанії
- Потреба та доступність у вивченні основ комп'ютерної безпеки збільшується

Social engineering

- 85% усіх кібер-атак стаються через людський фактор
- З часом нові технології важче зламати. Людська неуважність залишається однаковою
- Найбільш популярним видом кібер-атак залишається фішинг та імперсонація через пошту

Third-party exposure

- Кіберзлочинці шукають менш захищені мережі, які співпрацюють з основною ціллю хакера (приклад – злив даних 214 мільйонів користувачів Facebook та Instagram через Socialarks)
- Рестрикції через COVID-19 > популяризація фрілансу та аутсорсу > збільшення ризику кібер-атаки через менш захищених посередників
- 75% усіх кібер-атак 2020 року мали зв'язок з використанням застарілого, уразливого програмного забезпечення

Помилки конфігурації

- Не правильно налаштовані захисні протоколи / захисне програмне забезпечення робить компанію уразливою до кібер-атак
- Збільшений ризик при наявності інфільтраторів, які можуть розпізнати та повідомити про уразливість захисту

Невиконання правил безпеки

- 80% компаній мають внутрішні курси з кібер-безпеки, здебільшого з щорічною перевіркою
- Більшість кібер-атак з використанням людського фактору можна пов’язати з неповним дотриманням цих правил (перевірка антивірусу, включення VPN, регулярна зміна паролю, двох-факторна автентифікація, тощо)

Погана кібер-гігієна

- 60% усіх компаній не мають швидкої процедури знаходження/оновлення паролю у випадку забуття його працівником
- 42% компаній дозволяють та(або) практикують запис паролів на наліпки
- 54% компаній не використовують двох-факторну автентифікацію
- 37% працівників використовують двох-факторну автентифікацію поза межами компанії
- Лише половина працівників змінюють пароль одразу після кібер-атаки та третина змінює регулярно пароль (якщо це не є обов'язковим критерієм у компанії)

Уразливість Cloud-сервісів

- Звіт від IBM стверджує, що безпека Cloud-сервісів не збільшується – за останні 5 років кількість кібер-атак через ці сервіси збільшилися на 150%
- При збільшенні популярності використання Cloud-сервісів без значного покращення їхньої надійності – деякі звіти прогнозують збільшення цього виду кібер-атаки

Небезпека мобільних девайсів

- Збільшення вірусів та трекерів на мобільних пристроях
- Найбільша кількість атак спрямована на Android девайси
- Великий ризик при прошивці Apple (Jailbreak)
- Особлива небезпека при зберіганні паролів в нотатках, нівелює двох-факторну автентифікацію

Недостатня безпека IoT (smart house)

- 70% домів у США мають хоча б 1 IoT пристрій, популярність швидко росте по світу
- Протоколи безпеки від атак IoT пристроїв поки не встигають за темпами розвитку цих технологій

Ransomware-as-a-service

- Відносно новий фактор збільшення ризику кібер-атак
- З’являються компанії, які створюють віруси та дають їх слабким хакерам у обмін на відсоток з награбованого
- Це збільшує доступність людей з недостатньою експертизою до участі у кібер-атаках

Збереження баз даних

- Популярність баз даних збільшується разом з автоматизацією роботи з ними
- Збільшується ризик SQL ін’єкції
- Зміна пріоритету з кількості на якість зменшує відсоткову кількість SQL ін’єкцій серед видів кібер-атаки

Відсутність план дій при кібер-атаці

- Кожна компанія повинна мати свій департамент по кібер-безпеці та правила поводження з кібер-атакою
- Відсутність плану дій збільшує шанси на повторну кібер-атаку
- 21% європейських компаній все ще не мають систематизованого плану дій

Фактори збільшення ризиків

- Діджиталізація компаній
- Відсутність департаменту кібер-безпеки у компанії
- Збільшення популярності «програм-вимагачів»

Фактори зменшення ризиків

- Систематизація створення, оновлення та дотримання правил безпеки та їхній регулярний перегляд
- Популяризація курсів з кібер-безпеки в межах та поза межами компанії
- https://skillsforall.com/career-path/cybersecurity?userLang=en-US