USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА НАСТАВНИЦТВА ДЛЯ ТЕХНІЧНИХ ДИРЕКТОРІВ

ТЕМА 3. ВСТУП

Ця презентація була підготовлена на замовлення USAID. Її самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цій презентації, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

РОЗРОБКА ПРОГРАМИ НАСТУПАЛЬНОЇ КІБЕРБЕЗПЕКИ ДЛЯ ПРОАКТИВНОГО ВИЯВЛЕННЯ ТА УСУНЕННЯ ВРАЗЛИВОСТЕЙ

РОЗРОБКА ПРОГРАМИ НАСТУПАЛЬНОЇ КІБЕРБЕЗПЕКИ ДЛЯ ПРОАКТИВНОГО ВИЯВЛЕННЯ ТА УСУНЕННЯ ВРАЗЛИВОСТЕЙ

Згідно з Оксфордським словником англійської мови, термін «Наступальний» (Offensive) може визначатись як «активно агресивний; атакуючий». Проте, вислів «Найкращий захист – це напад» (який приписують Джорджу Вашингтону, 1799 р.) точніше передає сутність,

Яким чином це стосується кібербезпеки?

- Усі ми покладаємось на тактику, методи та процедури (ТМП)
  - Зловмисники користуються недоліками або слабкими місцями
  - Кібербезпека захищає активи
- Вразливими місцями можуть бути:
  - Люди (навчання, знання, тощо)
  - Процес (конфігурація, робочий процес, розробка, тощо)
  - Технологія (відомі / невідомі недоліки, порти / протоколи, програмні / апаратні помилки, тощо)

АТАКУВАТИ ЧИ НЕ АТАКУВАТИ

Нації можуть воювати, а уряди можуть заявляти про ворожі наміри.

Компанії та організації не є націями або урядами, вони не повинні:

- З власної ініціативи брати участь в кібератаках
- Використовувати принципи ТМП для відповіді на агресивні дії, направлені проти Вашої діяльності
- Впроваджувати наступальні можливості у свою діяльність

Метою сьогоднішньої теми є створення міцної системи захисту для запобігання атак проти Вас.

Більшість зловмисників звертають увагу на:

- Організації з поганим захистом, тому що їх легко атакувати і вони слугують потенційним виходом до іншої цілі
- Відомі вразливості та вразливості нульового дня, тому що вони можуть використовувати їх
- Ексфільтрацію даних, тому що вони можуть їх отримати та використати у своїх цілях пізніше
- Фішинг / атаки з метою вимагання

НАСТУПАЛЬНИЙ ЗАХИСТ ПОЧИНАЄТЬСЯ З ОБОРОНИ

Почніть з основ наступального захисту:

- Принципи, процедури та КПЕ
- Навчання є критичним
- Визначення вразливостей:
  - Постачальники та інші (уряди, індустрії, групи InfoSec) повідомляють
  - Використання сканерів для виявлення вразливості на регулярній основі
  - Перевірка конфігурації (сканери AWS, Azure, тощо, надані хостом для перевірки конфігурацій)
- Закрийте вразливі місця відповідно до ризику та частоти:
  - Критичні вразливості / вразливості з високим ризиком потребують негайного виправлення:
    - Закрийте порти, переналаштуйте програми, встановіть файрвол для захисту – виправлення без програмних патчів
  - Встановлення програмних патчів є обов'язковим:
    - Рекомендовані програмні патчі з критичним / високим рівнем розгортаються протягом 15 днів після релізу, з середнім / низьким рівнем – протягом 30 днів
    - Налаштуйте вікно патч-файлів для отримання нових файлів кожного місяця
    - Встановіть екстрений процес для позасмугового виправлення

НАСТУПАЛЬНИЙ ЗАХИСТ ПОЧИНАЄТЬСЯ З ОБОРОНИ - ПРОДОВЖЕННЯ

- Проскануйте на наявність інших слабкостей (non-patch):
  - Нові девайси / програми були додані до Вашої мережі
  - Відкритий спільний файловий ресурс
  - FTP-сайти (захищені та незахищені)
- Постійно навчайте користувачів:
  - Плакати та вивіски
  - Оновлення електронною поштою про інформаційно-психологічні атаки, невідомі телефонні дзвінки, активні фішингові кампанії, які спостерігають Ваші команди
  - Теоретичне навчання
  - Робота з дому
- Виправлення відомих недоліків, застаріле апаратне та програмне забезпечення, безпечні бібліотеки кодів, надійні репозиторії для вихідного коду
- Управління третьою стороною: формулювання договору, принципи, огляд захисту

РОЗУМІННЯ РИЗИКУ

- Розробіть програму для оцінки ризику:
  - Нове апаратне / програмне забезпечення
  - Нові сервіси (в масштабах організації)
  - Формулювання контракту – необхідна кібер мова
  - Вловлювання застарілих ризиків (існуюче апаратне / програмне забезпечення / сервіси / контракти).
- Співпрацюйте з іншими:
  - Управління кадрами – перевірка відомостей
  - Юридичний відділ – контракти
  - Закупівельний відділ – послуги
  - Тощо
- Повідомляйте менеджмент про ризики
  - Поясніть виявлений ризик менеджменту; повідомте їх про відповідальність / ризик
  - Продемонструйте, як ризик усувається або ні за допомогою звітних показників
  - Визначте пріоритет виявленого ризику

НАСТУПНІ КРОКИ…

Почніть сьогодні

- Використовуйте ресурси, які Ви маєте:
  - Особи, які можуть допомогти виявити критичний ризик
  - Повідомлення від постачальника
  - Встановлення патч-файлів
- Залучайте менеджмент
  - Пояснюйте невідомі ризики та чому їх розуміння важливе
  - Співпрацюйте з іншими відділами (юридичний, кадровий, тощо)
- Навчайте, навчайте та ще раз навчайте…
  - Проінформована культура прийматиме кращі рішення, але ніщо не ідеальне
  - Вони будуть виявляти слабкості, які Ви не зможете, вони будуть говорити та ділитись інформацією
  - Кожного разу, як вони роблять щось правильно, для Вашої команди на один потенційний інцидент стає менше

Залишились запитання…?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ДЯКУЮ