USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

CTO PEER MENTORING PROGRAM

TOPIC 3 MENTOR SESSION

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

DEVELOPMENT OF AN OFFENSIVE CYBERSECURITY PROGRAM FOR PROACTIVELY IDENTIFYING AND REMEDIATING VULNERABILITIES

DEVELOPMENT OF AN OFFENSIVE CYBERSECURITY PROGRAM FOR PROACTIVELY IDENTIFYING AND REMEDIATING VULNERABILITIES

According to Oxford Language, Offensive can be defined as "actively aggressive; attacking". Yet, the phrase "the best defense is a good offense" (attributed to George Washington in 1799) is more accurate,

How does it apply to Cybersecurity?

- We all rely on tactics, techniques, and procedures (TTP)
  - Bad actors to take advantage of flaws or weakness
  - Cybersecurity to protect assets
- Vulnerabilities can be:
  - People (training, knowledge, etc.)
  - Process (configuration, workflow, development process, etc.)
  - Technology (known / unknown flaws, ports / protocols, application / hardware errors, etc.)

ATTACK OR NOT TO ATTACK

Nations can go to war, and Governments can declare hostile intentions.

Companies & Organizations are not nations or governments and should never:

- Proactively engage in cyber attacks
- Use TTPs to respond to perceived offensive acts against your operations
- Design offensive capabilities into operations

The intent of todays topic is to build a strong defense, and to have that act as the reason to not attack you. Most attackers will go after:

- Poorly defended organizations because they are easy & potentially a gateway to another target
- Known and 0-day, vulnerabilities because they can exploit them
- Exfil of data because they can get it and it could benefit them later
- Phishing / ransomware attacks

OFFENSIVE PROTECTION STARTS WITH DEFENSE

Start with the basics for offensive protection:

- Policies, Procedures, and KPI's
- Training is critical
- Identifying vulnerabilities:
  - Vendor and others (Governments, industry, InfoSec groups) provide notifications
  - Using vulnerability scanners on a frequent basis
  - Configuration checks (AWS, Azure, etc. scanners provided by the host to verify configurations)
- Close vulnerabilities based on Risk and Frequency:
  - Critical / High Risk may need immediate fixes:
    - Close ports, reconfigure applications, place a FW to protect it – non-patching fixes
  - Patching should be done with out fail:
    - Recommend Critical / High patches are deployed within 15 days of release and Medium / Low within 30
    - Schedule a patch window for monthly patches
    - Establish an emergency process for out of band patching

OFFENSIVE PROTECTION STARTS WITH DEFENSE - CONTINUED

- Scan for non-patch weakness:
  - New devices / applications added to your network
  - Open file shares
  - FTP sites (secure and unsecure)
- Continuously educate users:
  - Posters and signs
  - Email updates about social engineering, strange phone calls, active phishing campaigns your teams are seeing
  - Tabletop exercises
  - Work from Home
- Fixing known flaws, end of life hardware and software, secure code libraries, trusted repositories for source code
- Third party management: Contract language, Policies, Review of protections

UNDERSTANDING RISK

- Establish a program to evaluate risk:
  - All new hardware / software
  - New services (organizational wide)
  - Contract language – required cyber language
  - Plan to capture legacy risk (existing hardware / software / services / contracts).
- Engage with others:
  - Human Resources – background checks
  - Legal – contracts
  - Procurement – Services
  - Etc.
- Report risk to Management
  - Explain identified risk to Management; Make them aware of responsibilities / risk
  - Demonstrate how risk is / isn't improving by reporting metrics
  - Prioritize identified risk

NEXT STEPS…

Start Now

- Utilize resources you have:
  - Individuals who can help identify the highest risk
  - Vendor notifications
  - Establishing a patch window
- Bring Management onboard
  - Explain the large amounts of unknown risk and why understanding is needed
  - Leverage other departments (legal, HR, etc.)
- Educate. Educate, Educate…
  - An informed culture will make better decisions, but nothing is perfect
  - They will spot weakness you can't, now they will know to speak up and share the information
  - Every time they do something right, it one less potential incident for your team

Questions … ?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

THANK YOU