Data Connectors’ Ohio Virtual Cybersecurity Summit

1: broken authentication- exploitability(as long as password(1962 was earliest)), prevalence(widespread-most application need authentication systems), high impact (usually granted everything)

-types of attacks: credentials stuffing- brute force attacks(can sell them on darknet, then sell and use them on other 3rd parties to see if use the same username and password and resell the on the darknet), password spraying- less sophisticated way of credential stuffing, injection attacks-authentication is bypassed(can access the admin account, session hijacking- attackers steals cookie and bypass the authentication, session ID url rewriting- atttackers rewrites url to bypass authentication,

-how to prevent: multifactor authentication, do not ship with default credentials,enforcestrong passwords, use breached password detection

2: real-time asset visibility and security for everyday devices

-tradtional- servers, workstation, laptops, tablets, networking deices

- newer- IoT, IoMT, OT(50billion devices in 2025)

- legacies devices htay may have been deployed and don’t know

-difficult to scan and patch

- no security agents

-sheer volume of devices

-these networks are coverging

-why now?

-mirai botnet (IoT)

Hackable ST Jude cardiac devices (IoMT)

Chinese manufacturers (banned)

Ripple20 vulnerabilities

Solarwind vulnerabilities

* Passive discovery is preferred vs active scanning,
* Realtime an granular device content
* Know how devices are behaving
* Network segmentation is critical
* Flexible segmentation approach
* Connected device security required collaboration

Endpoint management and security

* Device in offices have not been used in months
* New windows versions
* New adobe updates multiple per months
* cyberattack and phishing quadrupled
* what are our target groups?
  + Platforms to support
    - Xp to windows 10
    - Microsoft devices
    - servers
  + Different schedules in different departments
    - Noncritial
      * Can be restarted
      * No or low s=risk
      * User interactio
    - Critical
    - Servers
  + Different level of interaction
    - Self service approach
    - Locked systems
    - Test devices and pilot users
* Where do we go from here?
  + Stick with Work From Home
    - Inventory & vulnerabilities
    - Application and patches/updates
    - Encryption
  + Back to office
    - Inventory and vulnerabilities
    - Patching and updates
    - Backups and devices
  + Hybrid
    - Scheduling
    - Patching and updates
    - Backups and devices
* Mitre att&ck for assessing and mitigation
  + Main components(you, the attacker, and controls
    - Adversary emulation planning on mitre
      * Threats against your business
    - Attack matrixs
      * techQues they leverage
      * preparation- company, users, OS, Applications (choose techniques based off these)
      * stop relaying on techniques and rely on the tactics, shift in prioritization, improved risk reduction and assessment.
      * Asset hardening/it hygiene, attack surface reduction (disabling functionality, zero-trust technologies and policies
    - shield matrix(mitigation)
      * Defenses to counter attacks