Cybersecurity for Local Governments and Schools

A Weekly Cybersecurity Awareness Month Web Series

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 3 – Protecting Against Unseen Dangers

Richard Saunders, IT Specialist
Division of Local Government and School Accountability

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Categories

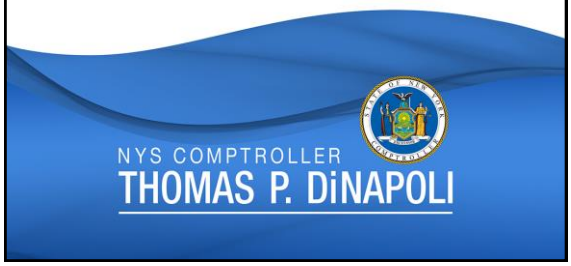
- Personal, Private and Sensitive Information
- IT Asset Inventories
- Policies and Procedures
- IT Security Awareness
- Written IT Agreements
- Website Content
- Internet Use
- Malicious Software
- User Accounts and Permissions
- Passwords
- **Networks and Computers**
- **Wireless Access**
- Physical Access
- Disaster Recovery
- Audit Trails and Logs

Recap - Week 2

- Website content
- Internet use
- Malicious software
- User Accounts and Permissions
- Passwords

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Networks and Computers



Impact on the CIA Triad

- Confidentiality
  - Unauthorized disclosure of personal, private, or sensitive information
- Integrity
  - Cyber vandalism
  - Fraudulent manipulation of data
- Availability
  - Denial of service
  - Ransomware

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Software Vulnerabilities

- The Software Vulnerability Lifecycle:
  - Research - Discovery - Disclosure / Patch Release.
  - Research – Discovery - Disclosure / Patch Release - Patch Applied - Exploit Developed
  - Research – Discovery - Disclosure / Patch Release - Exploit Developed - Patch Applied?
- Website: https://cve.mitre.org
  - Publicly available database of known cybersecurity vulnerabilities
- Website: https://www.exploit-db.com
  - Publicly available database of exploits and corresponding vulnerable software

Open Port Management

- What is a port?
  - Ports act like P.O. boxes for a computer.
  - Not all open ports are bad.
  - Some are riskier than others.
  - Some are known to be used by malicious software.
- Firewalls can help.
  - Host-based firewalls installed on each host connected to the network can mitigate risk
  - Whitelisting versus blacklisting
- Preventive port scanning:
  - Know which ports are open on your system before the criminals do.
  - Many open-source and commercial tools are readily available.

Network Segmentation

- Make use of security zones.
  - Classify resources based on which zone they belong in.
- Enforce the principle of least privilege.
  - Users only have access to the minimum resources needed in order to complete their job functions.
- Separate guest / low security networks:
  - Vendors / contractors
  - Students
  - IoT / BYOD equipment
- Prevent privilege escalation / lateral movement.
  - Attackers rarely start with admin access.

Networks and Computers – Best Practices

- Change default configurations to appropriately meet security needs.
- Leverage firewalls to effectively control what traffic is allowed on the network.
- Ensure that sensitive systems are not accessible from the internet.
- Consistently monitor systems that are required to be internet-accessible.
- Apply system and software updates automatically or in a timely manner.
- Identify vulnerabilities through proactive self-scanning.
- Restrict high-risk or unnecessary ports and services.
- Restrict the use of personal devices on the network.
- Ensure sufficient segregation between private networks and guest/student/vendor networks.
- Configure network devices to automatically lock or end the session after a predetermined length of time.

Wireless Access

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Impact on the CIA Triad

- Confidentiality
  - Wireless eavesdropping
- Integrity
  - Wireless hijacking / wireless redirection attacks
- Availability
  - WiFi jamming attacks

Rogue Devices / Access Points

- What is a rogue device?
- Rogue access points:
  - False access points set up by attackers
  - May have the same "name" (SSID) as a legitimate access point
  - Devices tend to remember access points and may inadvertently auto-connect to a rogue access point.
- Detection Methods:
  - Go for a walk and follow the signal!
  - Open source and commercial tools are available for detecting wireless access points.
  - Compare what is detected with an inventory of managed assets.

Man-in-the-Middle Attacks

USER ⟷ SERVER

USER ⟷ ATTACKER ⟷ SERVER

- A user thinks they are connected to a legitimate server.
- The server also thinks it is communicating with a legitimate user.
- Attackers can both manipulate and eavesdrop on the data as it is transmitted between the two parties.
- Home offices are especially susceptible.

WiFi Jamming Attacks

- Signal Jamming:
  - Can be unintentional: Bluetooth and microwaves can interfere with WiFi signals.
  - Can be malicious: Bursts of strong RF signals can make WiFi channels unusable.
  - Jamming devices are often costly, illegal, and hard to obtain.
- Malicious Traffic:
  - Packet flooding
  - De-authentication attacks
  - Same basic effect as a signal jammer, easier to execute
- Possible indicator of a larger attack
- WiFi jamming in the news – Secaucus, New Jersey – April 2019

Wireless Access – Best Practices

- Do not conduct sensitive business over WiFi.
- Keep an accurate inventory of wireless devices.
- Be security conscious when WiFi browsing:
  - Look for the "s" in https://.
  - Unsecured http:// pages may be an indicator of a rogue connection.
- Change the defaults.
  - Network name (SSID)
  - Administrator credentials
- Limit the signal.
- Make use of strong encryption.
- Segregate guest/student/vendor WiFi access from the private network.
- Take steps to ensure that users are not allowed to connect unapproved devices to the network.

Sneak Peek - Week 4

- Physical Access
- Disaster Recovery
- Audit Trails and Logs

Thank You

Division of Local Government and School Accountability
LGSAAppliedTech@osc.ny.gov