Cybersecurity for Local Governments and Schools

A Weekly Cybersecurity Awareness Month Web Series

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 2 – WE Are Our Own Biggest Threat

Mandy Hopkins, IT Specialist
Karen Stewart, Auditor 2
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 1

- Personal, Private and Sensitive Information
- IT Asset Inventories
- Policies and Procedures
- IT Security Awareness
- Written IT Agreements

NYS COMPTROLLER THOMAS P. DiNAPOLI 4

Website Content

NYS COMPTROLLER THOMAS P. DiNAPOLI

Website Content

- Threat
  - Inadvertent disclosure of personal, private or sensitive information
- Attack
  - Data breach: Illinois Department of Employment Security (May 2020)
  - Website Data Breach: Philadelphia Department of Public Health (October 2019)
- Best practice
  - Periodically review municipal and third-party websites for sensitive information disclosure.

NYS COMPTROLLER THOMAS P. DiNAPOLI 6

Website Content

- How your sensitive information is found/disclosed on your website(s):
  - Simply browsing online
  - Website incorrectly configured
  - Identified a web vulnerability
- What can be done with the information disclosed:
  - Identity theft
  - Potential compromise of online accounts
  - Use social engineering to access more information
  - Fraud

Website Content

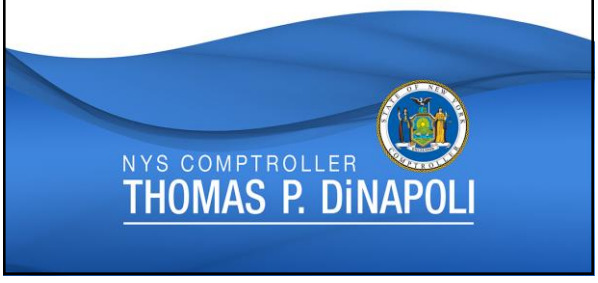
- NYS Information Security Breach and Notification Act:
  - State entities and persons or businesses conducting business who own or license computerized data which includes private information must disclose any breach of the data to New York residents whose private information was exposed.
- Under section 208 of the State Technology Law:
  - A state entity must also notify the three following NYS offices: the NYS Attorney General (AG), the NYS Office of Information Technology Services, and the Department of State's Division of Consumer Protection.

Website Content

Personal, Private, Sensitive Information (PPSI):

Is any information which – if subjected to unauthorized access, disclosure, modification, destruction, or disruption of access to or use – could severely affect critical functions, employees, customers, third parties, or citizens of New York in general.

Internet Use



Internet Use

- Threat
  - Inadvertent exposure to network or computer compromise
- Attack
  - Network infection: U.S. Geological Survey (October 2018)
- Best practice
  - Monitor employee Internet use and enforce the municipality's acceptable use policy.

Internet Use

- High Risk Internet Activity
  - Viewing pornography
  - Conducting unlawful activities
  - Downloading pirated software
  - Online gaming
  - Online shopping
  - Accessing personal email
  - Paying personal bills
  - Visiting personal social media, etc.

Internet Use

- How information is exposed:
  - PPSI is exposed inadvertently on fraudulent websites or clicking on ads
  - Financial transactions done online
  - Phishing Email accounts/Social media accounts
  - Eavesdropping on transactions through Man-in-The-Middle
- Cybercriminals want this valuable data for:
  - Unauthorized transactions/access
  - To sell
  - Impersonation
  - Identity theft

Malicious Software

Malicious Software

- Threat
  - Malicious software infections on municipal networks and computers
- Attack
  - Computer infections: Bixby Public Schools, Oklahoma (December 2019)
- Best practice
  - Ensure all municipal computers have malicious software protection that frequently downloads new definitions and runs full scans.

Malicious Software

- Malware can:
  - Alter, corrupt, or delete files, or erase entire drives
  - Cause computer booting issues & corrupt applications
  - Capture and send sensitive information to attackers
  - Access and use email accounts to spread
  - Simply lay dormant until summoned by an attacker.

NYS COMPTROLLER THOMAS P. DiNAPOLI 16

Malicious Software

- Trojan Horse
- Virus
- Worm
- Adware
- Spyware
- Ransomware
- Rootkits

NYS COMPTROLLER THOMAS P. DiNAPOLI 17

User Accounts and Permissions

NYS COMPTROLLER THOMAS P. DiNAPOLI

User Accounts and Permissions

- Threat
  - User account misuse or unauthorized user accounts
- Attack
  - Former employee access: Harrison Township School District, New Jersey (February 2020)
- Best practice
  - Periodically evaluate network, computer and application user accounts and permissions, and disable or remove any deemed necessary.

User Accounts and Permissions

- Unnecessary User Accounts
  - Can be network, local or application level user account
  - Create additional work to manage and risk errors, resulting in inadvertently granting more access than necessary
  - Are subject to misuse and unauthorized use
    - Example: No longer employed

User Accounts and Permissions

- Default User Accounts (not renamed)
  - Default admin accounts are the riskiest default account
  - Default guest accounts are also a risk
  - Default financial system and SIS accounts

User Accounts and Permissions

- Improperly Shared or Generic Accounts
  - Shared accounts make it difficult to link suspicious activity to one user.
  - While some generic accounts may be necessary for services, others such as BldgGuest may not be.

User Accounts and Permissions

- Administrative Accounts
  - Lesser-privileged accounts should be created for non-administrative functions, such as Internet browsing or checking email.
  - Higher-privileged accounts are targeted.

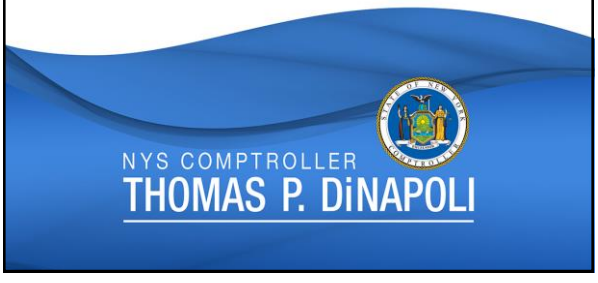
User Accounts and Permissions

- Unnecessary Administrative Permissions
  - Can be network, local or application level (financial and SIS)
  - Local user accounts with administrative permissions have full control of the computers on which those accounts reside.
  - Admin permissions should be revoked when an employee leaves or be modified if they change positions.

User Accounts and Permissions

- Unnecessary User Permissions
  - Should be based on job duties
  - Can be network, local or application level (financial and SIS)
  - User permissions should be revoked when an employee leaves or modified if they change positions.

Passwords



Passwords

- Threat
  - User account compromise
- Attack
  - Wallpaper change: Paul R. Smith Middle School, Florida (April 2015)
- Best practice
  - Require passwords to contain at least eight characters, meet complexity requirements and be changed every 60 days or less.

Passwords

Strong passwords improve chances that unauthorized users will be prevented from accessing computer systems, because guessing or cracking long, complex passwords takes far longer than short, simple passwords.

For example, a 4 character password containing uppercase and lowercase letters only has approximately 7.3 million possible combinations.

In contrast, an 8 character password containing uppercase, lowercase, numeric and special characters has nearly 900 trillion possible combinations.

Using a standard password-cracking mechanism, which is capable of testing one million combinations per second, the simple 4 character password could be cracked in just over 7 seconds while the complex 8 character password could take more than 28 years!!!

Sneak Peek - Week 3

- Networks and computers
- Wireless access

Thank You

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