Software Management

Cybersecurity Awareness Month
October 2022

New York State Comptroller
THOMAS P. DiNAPOLI

1

Division of Local Government and School Accountability

Applied Technology Unit
Ariel Bethencourt

New York State Comptroller
THOMAS P. DiNAPOLI

2

Software

Maintaining properly supported and updated software helps to bolster your posture against cybersecurity threats.

- Software used in local governments could include:
  - Financial;
  - Utility;
  - Payment; and
  - Operating systems.

New York State Comptroller
THOMAS P. DiNAPOLI

3

Software Updates

- All software and hardware devices need occasional updates for improved performance, compatibility and security.

Software Patches

Patches are operating system and other software updates

- Patches can:
  - Add features;
  - Fix performance bugs;
  - Install new hardware drivers;
  - Update to address newly identified vulnerabilities and stability problems.

Software Patches (continued)

- When software patches are not installed timely, your municipality's network, connected devices and any data contained within are at an increased risk of vulnerability due to increased exploitable gaps in your operations and of compromise or disruptions due to:
  - Malware, such as ransomware, and
  - Operational instability or incompatibility.

Actions to Update Software

- Updates may be:
  - Automated and notify users when updates are available to download and install;
  - Manual and require users to remain informed of security vulnerabilities and the remediating updates made available in security bulletins to download and install.

Actions to Update Software
(continued)

- Enable automatic updates whenever possible.
  - Helps to ensure that software updates are installed in a timely manner.
- Manual updates require action to search and obtain the vendor's update, download and install.

Cautions

- Only download software updates from trusted vendor websites, rather than through email links or pop-ups.
- Ensure you use a trusted network when downloading or installing software updates.
- Do not use software that is no longer supported by the vendor (unsupported software).

OSC Audit Findings

Our audits have identified software management-related findings.

- As appropriate, these findings can be found in our publicly issued reports.
- When of a sensitive nature, we communicate those findings confidentially to officials.

OSC Audit Findings
(continued)

- Common software management-related findings:
  - Lack of comprehensive written policies and procedures;
  - No, or untimely, software updates;
  - No, or inadequate, software inventory.

Additional LGSA Resources

Visit our website for additional cybersecurity resources:

- Publications
  - https://www.osc.state.ny.us/local-government/publications
- Training
  - https://www.osc.state.ny.us/local-government/academy

Additional LGSA Resources
(continued)

Visit our website for additional cybersecurity resources:

- Audits
  - https://www.osc.state.ny.us/local-government/audits

Other Resources

- Center for Internet Security (CIS)
  - https://www.cisecurity.org/
- Cybersecurity and Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/
- Federal Bureau of Investigation (FBI)
  - https://www.fbi.gov/investigate/cyber

Other Resources (continued)

- National Institute of Information Technology Services (NIST)
  - https://www.nist.gov/cybersecurity
- New York State
  - Office of Information Technology Services
    - https://www.its.ny.gov
  - Division of Homeland Security and Emergency Services
    - https://www.dhses.ny.gov/cyber-incident-response-team

Questions?

Contact us

- LGSA Applied Technology Unit's Cyber Team
  - LGSACyberTeam@osc.ny.gov
- LGSA Help Line
  - 1-866-321-8503 or
  - 518-408-4934

New York State Comptroller
THOMAS P. DiNAPOLI

16

Thank You!

New York State Comptroller
THOMAS P. DiNAPOLI

17