ANDREW W.
MAYLOR
COMPTROLLER

Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

STATEWIDE CYBERSECURITY RESPONSE TEAM

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
TELEPHONE (617) 727-5000
WWW.MACOMPTROLLER.ORG

CYBERSECURITY LESSONS LEARNED

Last Updated: August 13, 2019

Overview

Over the past few years cyberattacks against organizations, from large government Departments to small businesses, have been steadily growing, with hackers specifically targeting employees (phishing). And, while denial of service (DoS) attacks are still a leading form of cyber-crime, ransomware, malware and social engineering attacks are becoming more prominent in our workplace. The Commonwealth has engaged expert firms to help remediate several of these unfortunate cyber incidents and advise Departments of the proper policies and procedures to improve overall cyber hygiene. Below are some lessons learned to assist Departments with building appropriate cyber security protections and strategies.

Department Related Observations

1. All state employees need continuous training on their role in preventing cyber-attacks.
2. Departments have varying degrees of sophistication in IT infrastructure, number and skillsets of IT staff.
3. Use of separate networks reduces the risk for financial and banking functions.
4. Some Departments lack detailed network diagrams, user access management and IT inventory controls. Departments that have conducted assessments for Payment Card Industry (PCI) compliance for accepting credit cards and other security assessments are better positioned for expedited containment in a cyber event with updated Department documents.
5. Department Security Officers (DSOs) could benefit from additional training on the business purposes of security roles and how to evaluate roles to ensure sufficient access with appropriate segregation of duties.

Report Cyber Incidents to: CTREmergencyNotification@mass.gov

CYBERSECURITY LESSONS LEARNED

6. Segregating and securing Personally Identifiable Information (PII), sensitive and confidential data in accordance with state and federal privacy laws, are mandatory internal controls for all Departments for legal and fiscal compliance due to the extreme costs to mitigate data breaches.

Cybersecurity Recommendations – The Top Two

1. **Security Awareness Training**. Research shows that phishing is the leading cause of cyber attacks*. Provide continuous security awareness training to all staff and contractors on the latest cyber threats and red flags. Tips:
    - Do not "enable macros/content" in email attachments
    - Do not enter credentials (user names/passwords) for requests based upon links in emails
    - Verify the source for any requests to change high risk items, such as bank accounts, payment addresses, EFT or direct deposits etc.
2. **Continuous Updating and Patching Protocol**. *"Given that the majority of victims are breached because of unpatched known software vulnerabilities, effective vulnerability response is a critical weapon in the cybersecurity arsenal."* ** Keep servers, desktops, operating systems and third party applications up to date with anti-virus software and security patches/updates as to ensure that vulnerabilities are not created or exploited. Patching programs and policies should include third party applications and printers.

*Digital Guardian. "91% of cyber attacks start with a Phishing Email: Here's How to Protect Against Phishing"

**Ponemon Institute "Today's State of Vulnerability Response: Path Work Demands Attention"

Strategic Recommendations

3. **Incident Response Plan**. Have an updated incident response plan that clearly identifies the resources and processes should a cyber-incident occur. As part of the Department Internal Control Plan include an updated Incident Response Plan that clearly identifies the resources and processes that could potentially be impacted, and a plan of containment and remediation, should a cyber-incident occur. In addition, the Incident Response Plan should have a process

Report Cyber Incidents to: CTREmergencyNotification@mass.gov

if a cyber-incident occurs to keep artifacts and copies of compromised files, screen shots and other logs in separate repository for forensics investigation.

4. **Risk Assessments and Internal Controls**. As part of the required Internal Control Plan, Departments should conduct a risk assessment to identify the data and systems assets that need to be maintained and secured from a cyber-incident. The Department should also develop a strategic plan to continually monitor and secure these assets from cyber-threats.

5. **Department Security Policies**. Draft and implement Department data management and system security policies. Executive Departments are required to follow the Enterprise Security Policies issued by the Executive Office for Technology, Security and Services. (EOTS). Non-Executive Departments are required to follow either the EOTS Enterprise Security policies as the default Commonwealth standard or comparable Department standards as part of their Internal Control Plans. See: **EOTSS Enterprise Security Policies and Standards.**

6. **Asset and Data Security Management.** Maintain a centralized asset management system to track internal assets, their locations, and the asset owners. Properly identify and secure (encrypt, store) confidential data separate from other operational data. Unsecured sensitive and confidential data that resides on PCs, networks, servers, mobile devices can be breached if these assets are compromised. Every Department should have a data management policy and plan to encrypt this data, securely manage the encryption keys, and manage the lifecycle of the encryption keys.

7. **Network Documentation**. Department networks and devices are fluid. The Department should always keep network diagrams, data flows and records of updates current, which improves the ability to properly patch and keep applications up to date, as well as assisting with remediation in a cyber incident.

8. **Secure Transmission**. Disable macro scripts from office files transmitted over e-mail. Encrypt all emails with PII, sensitive or confidential data.

9. **Software Restrictions**. Implement software restriction policies or other controls to prevent programs from being executed from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

10. **Access Management.** Local administrative rights should not be present on users' computers. Limit the use of shared privileged accounts and remove unused accounts. Define users and machine configurations in different user groups based on their roles so that appropriate group policies can be applied. Perform a regular audit of Active Directory permissions.

Report Cyber Incidents to: CTREmergencyNotification@mass.gov

CYBERSECURITY LESSONS LEARNED

11. **Contact the FBI** (at www.IC3.gov). Report suspicious email addresses, bank account change requests on where funds were, or were attempted to be, redirected. The FBI collects information about cyberattacks, successful breaches and cyber-attack attempts.

12. **Contact Banks**. Department banks should be notified in the event of a cyber-incident to alert them to the incident and ensure that access to online banking systems are suspended until a due diligence review confirms that there is no threat.

13. **Contact Local Police**. Local law enforcement should be contacted to log an official report.

14. **Mandatory State Reporting**.

    a. MGL Chapter 93H, and its corresponding regulations (201 CMR17.00), require reporting to the Attorney General and the Director of Consumer Affairs and Business Regulation of any *"known security breach or unauthorized use of personal information."*

    b. Chapter 647 of the Acts of 1989 requires that *"…variances, losses, shortages or thefts of funds or property shall be immediately reported to the state auditor's office…"*

Technical Recommendations

1. **Layered Virus and Malware Protections.** Implement a full-featured virus and malware protection software suite that offers layers of protections, such as signature recognition and behavioral detection heuristics capabilities, across the entire infrastructure - including all endpoints and mobile devices - and update frequently. Behavioral detection anti-virus options are superior to signature based antivirus options.

2. **DID - Defense in Depth (DiD).** Defense in Depth is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. If one mechanism fails, another mechanism provides redundant protection to control the threat.

3. **Restrict Usage of Server Message Block (SMB).** These ports should be closed for workstation end points.

4. **Deprecate (Replace) Unsupported Hardware and Software.** Upgrade to the latest supported servers, operating systems and applications.

Report Cyber Incidents to: CTREmergencyNotification@mass.gov

CYBERSECURITY LESSONS LEARNED

5. **Separation of Networks**. Use separate network connections for processing financial and banking transactions - not connected to the email system or general internet traffic.

6. **Monitor Network Traffic.** Limit traffic between servers and workstations to only necessary protocols. Expand visibility of traffic by monitoring outbound and inbound network flow. Implement data loss prevention ("DLP") monitoring to protect financial information, employee and student PII (Personally Identifiable Information), HIPAA (patients' health information), etc.

7. **Limit Domain and Network Administrator Accounts.** Routinely review and update domain administrator accounts. Remove any unnecessary accounts and limit solely to authorized personnel.

8. **Configure VPN and Remote Access.** VPN tunnel policies should restrict access for hosts and networks based upon the "principal of least privilege."

9. **Apply Best Practice Password Policies.** "Length is Strength". Enforce maximum password length and complexity. Long phrases with special characters are best. Change passwords frequently. Do not publish password formats.

10. **Multi-Factor Authentication (MFA).** Use multifactor authentication (each user is granted access only after presenting two or more pieces of identification) wherever possible, particularly with administrators accessing servers. If possible, add MFA to any administrator access in the environment to assure that administrative actions are conducted by authorized personnel only.

11. **Firewalls.** Network traffic should go through a security device (such as a firewall) that employs web filtering. Setup security devices to block end users from accessing threatening web sites.

12. **External Facing Internet Protections.** (DMZ and Firewall) Public facing servers should be separated on their own subnet which has its own firewall to protect from internet threats. An attacker who gains access to hosts within a DMZ, finds it much more difficult to gain access to hosts that reside on the internal networks.

13. **Group Policies**. Implement group policies that are applied to all Department computers upon log in. These group policies, with cyber security in mind, prevent end users from executing threatening actions on the agency network.

Report Cyber Incidents to: CTREmergencyNotification@mass.gov

CYBERSECURITY LESSONS LEARNED

14. **Back Up Files and Avoid Paying Ransom**. Back up servers and files frequently (for production servers – up to several times during the day); backups should then be saved both locally and offsite (daily offsite is preferred). If a server or its data is impacted by a cyber-event the server can be rebuilt and restored from a recent, non-impacted backup version. Avoid paying ransomware as payment does not guarantee recovery of intact files.

15. **Vulnerability and Penetration Testing**. Conduct regular independent vulnerability assessments and penetration testing to determine weaknesses in networks/end-point devices and whether sensitive data is sufficiently protected.

16. **Intrusion Detection (IDS) and Intrusion Protection (IPS).** IDS and IPS capabilities guard against known threats and zero-day exploits, SQL injection attacks and other web application attacks. IDS technology detects vulnerability exploits against a target application or computer while IPS technology adds the ability to block those exploits.

Cyber Security Resources:

- PRF56DesignatedOSC Data Security Statewide Contract with cyber resources to assist with risk assessments, vulnerability assessments, emergency incident response and mitigation, management, forensics, Payment Card Industry (PCI) compliance (if Department accepts revenue through credit cards.
- Payment Collection Data Security Policy
- Enterprise Information Security Policies and Standards | Mass.gov (Commonwealth Standard)
- Top 20 Critical Security Controls for Cyber Defense. Developed by the SANS Institute together with the Center for Internet Security (CIS) and other organizations.
- Federal Department of Health and Human Services (HHS) https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html (Departments accepting federal funds may be required to meet federal requirements). (See Interactive Cybersecurity Awareness Training)
- U.S. Security Awareness.org free resources. http://www.ussecurityawareness.org/highres/free-resources.html
- Center for Internet Security https://learn.cisecurity.org/ms-isac-registration
- Poneman Institute – Separating the Truths from Myth in Cyber security Report.

Report Cyber Incidents to: CTREmergencyNotification@mass.gov