NEW YORK STATE REGIONAL INFORMATION CENTERS

RANSOMWARE PROTECTIONS

This resource is designed to provide educational agencies with recommendations for technical controls and management processes to help protect against ransomware infection. Although these protections are focused on ransomware, many are applicable to other types of cybersecurity threats as well.

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In many cases, sensitive information may also be exfiltrated from the district with the threat that it be released publicly as a means of extorting payment.

SYSTEM PROTECTION REMINDERS

VULNERABILITY **MANAGEMENT**

Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.

SYSTEM **BACKUPS**

Ensure backups for critical systems are in place and audit backups for completion and functionality.

SYSTEM **HARDENING**

Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.

IDENTITY **MANAGEMENT**

Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.

APPLICATION **SECURITY**

Only use district approved softwares, audit system access, and isolate critical infrastructure.

Ensure ALL staff members are trained regularly on Data Security best practices, particularly **Email Phishing Recognition.**

CISA recommends agencies focus on the following prioritized investments:

- *Multi-factor Authentication*
- *Patch Management*
- *Backups Management*
- *Exposure Management*
- *Incident Response Plans*
- *Training Program*

PROTECTING OUR FUTURE REPORT:
https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c.pdf

***Updated:** September 2023*

VULNERABILITY MANAGEMENT

Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.

	DESCRIPTION	NOTES
PATCH MANAGEMENT	Patch known vulnerabilities that apply to all systems, software, and components in your environment.	Critical systems should be prioritized, however; all systems should be patched in the recommended timeframe. End of Life (EoL) systems should be retired whenever possible.
HARDWARE INVENTORY	Keep an inventory of authorized devices and detect unauthorized devices.	Know what devices are connected to your network at all times so they can be monitored.
SOFTWARE INVENTORY	Keep an inventory of authorized software and detect unauthorized software.	Know what software is in use so you can be sure it is secured and patched appropriately.
NETWORK PORTS	Limit and control network ports.	Ensure ports no longer in use are closed and open ports are limited in scope where possible.
WIRELESS ACCESS CONTROL	Secure and segment wireless networks, including elimination of open networks.	Guest networks should not have access to networked resources.
DEACTIVATE ACCOUNTS	Deactivate the user accounts of those no longer in need of access, including former employees.	Accounts of inactive users are often exploited as warning signs are less likely to be noticed.

FIVE STEPS FOR MANAGING SYSTEM VULNERABILITY

SCAN

Perform weekly external and internal network scans

PLAN

Deploy and implement an alert mitigation plan

PRIORITIZE

Make patches and fixes a high priority

VALIDATE

Test and validate patches and fixes before deployment

DEPLOY

Apply validated patches and fixes as soon as possible

SYSTEM BACKUPS

Ensure backups for critical systems are in place and audit backups for completion and functionality.

	DESCRIPTION	NOTES
BACKUP CREDENTIALS	Only accounts needed for backup operations should be able to connect to backup storage systems.	Backup systems should be kept as isolated as possible to prevent the spread of infections to backups.
DOMAIN BACKUPS	Backup servers should not be bound to the district domain.	Isolating backup servers from the domain prevents the spread of malware to the backup server via compromised domain credentials.
FILE SYSTEMS	Leverage different file systems for backup storage when feasible.	Machines running Linux often function as backup repositories.
OFFLINE STORAGE	One of the best defenses against propagation of ransomware encryption to the backup storage is to have offline storage.	Examples: • Replicated VMs • Storage snapshots • Cloud Connect backups • Rotating (Media) • Off-Network Sites
REGULAR TESTING	Test backups and systems on a regular basis.	Monitoring backups for completion and regularly conducting test restores helps ensure backup integrity.
BACKUP LOGS	Document and maintain a log of all system backups, testing schedules, and retention periods.	Accurate log documentation can greatly increase recovery time.
CURRENT IMAGE	Keep and maintain an up-to-date image for machines to assist in recovery.	Affected machines will likely need to be re-imaged as part of the recovery process.
FILE STORAGE	Store files on network shares or cloud systems where they can be backed up.	Files stored on workstations will likely be lost during restoration.

BACKUP PROCEDURES

- **IDENTIFY** the high value and/or critical systems that need to be backed up regularly
- **DETERMINE** who is responsible to create, maintain, and test scheduled backups
- **CREATE** and implement a backup schedule for critical and high value systems
- **TEST** backups and backup recovery and restoration procedures at defined periods

SYSTEM HARDENING

Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.

	DESCRIPTION	NOTES
ENDPOINT PROTECTION	Ensure NextGen anti-virus software is installed on all systems and up to date.	Endpoint Detection and Response (EDR) capabilities are highly recommended for prevention and recovery.
MANAGEMENT TOOLS	Remove or harden high-privilege, system management tools, such as PowerShell, wherever possible.	Attackers will often leverage existing tools in the environment to carry out attacks.
DOMAIN CONTROLLERS	Do not install additional software on domain controllers. Do not install additional non-critical roles.	Only mechanisms required for functionality and security should exist on domain controllers.
SECURE ADMIN WORKSTATION	Use a dedicated Secure Admin Workstation (SAW) to perform administrative tasks.	Day-to-day office work (e.g. email, web usage, etc.) should be conducted on a separate machine.
ENABLE DOMAIN AUDIT LOGS	Enable Audit Policy Settings with Group Policy.	See the **Appendix A: Audit Policy Settings** page for recommended settings.
SERVER MESSAGE BLOCKS	Disable outdated file and print sharing protocols Server Message Blocks Version 1 & 2 (SMBv1&2).	Use SMBv3 or higher.
OPERATING SYSTEM UPDATES	Apply critical and security patches within 1-3 weeks.	Prioritize updates on critical systems and infrastructure and externally accessible systems.
OPERATING SYSTEM FIREWALL	Limit and control system firewall ports.	Ensure ports no longer in use are closed and open ports are limited in scope where possible.
LOCAL ADMINISTRATOR PASSWORD SOLUTION	Utilize LAPS for the local management of domain computers.	LAPS is a Microsoft tool that sets a unique password for every local administrator computer account and stores it in Active Directory.

IMPROVEMENT ROADMAP

DEFINE Activities and Functions

AUTOMATE Wherever Possible

INCREASE Visibility into Systems

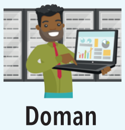
INVEST in Improving Expertise

VERIFY Activities are Performed

IDENTITY MANAGEMENT

Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.

	DESCRIPTION	NOTES
APPROPRIATE PERMISSIONS	Ensure accounts have appropriate permission levels.	Privileges to install software or applications should be limited to those who explicitly require it.
DOMAIN ADMINISTRATORS	There should be no day to day user accounts in the Domain Admin group.	Privileged users should have 2 Active Directory accounts: 1. Day to day work and office functions with no admin privileges 2. Privileged account that is used exclusively for tasks requiring administrative level permission
LEAST PRIVILEGED ACCESS	Follow the Least Privilege Access model for assigning account permissions.	All users should log on with an account that has the minimum permissions required for their work.
ADMINISTRATOR ACCOUNTS	The Domain Administrator account should exclusively be used for the domain setup and Domain-related disaster recovery.	Domain Administrator account credentials should be an exceptionally strong password and stored in a highly secure location.
PASSWORD POLICY	Update password policies to reflect best practices.	Recommendations: • Minimum 12 characters • Enforce password complexity • Enforce periodic changes
PASSWORD USE	Enforce password history should be set to 24 (or the maximum valued allowed by the system)	Passwords from older data breaches are being leveraged in current attacks.
MULTI-FACTOR AUTHENTICATION	Multi-factor authentication should be used with all Privileged accounts, VPN accounts, and all Email accounts.	Multi-factor authentication provides additional verification on the identity of the user.
SERVICE LOCKDOWN	Service accounts should only have the necessary access levels required for their specific tasks.	Reasons for the service account existence should be noted.

MULTI-FACTOR AUTHENTICATION	PRIVILEGED ACCOUNTS	PRIORITY TARGETS	EXTERNAL NETWORK ACCESS	HIGH - VALUE TARGETS
	 Doman Administrator	 Email	 VPN Access	 Banking Transactions

APPLICATION SECURITY

Only use district approved softwares, audit system access, and isolate critical infrastructure.

	DESCRIPTION	NOTES
SYSTEM ISOLATION	Required legacy systems and applications that rely on EoL software or do not allow for up-to-date patching should be isolated from other systems.	These systems should have internet connection disabled or limited in scope, documented mitigating controls, and should retired when possible.
USE APPROVED SOFTWARE	Know what systems are in use in your district so protections can be put in place.	Technology management tools should be vetted before use.
ACTIVELY MONITOR SYSTEM LOGS	Monitor, aggregate, and examine system logs for signs of compromise on a continuous basis. Critical logs should be accessible during an event.	Examples: • Repeated failed logins • Logins from strange locations/IPs • Logins at unusual hours • Users performing atypical tasks • Privileged account activity
PASSWORD REUSE	Login credentials should not be used across multiple systems.	Compromised credentials are often used to attempt to access other systems.
REVIEW ACCOUNTS	Review Accounts regularly to ensure they need to remain active.	Focus on newly created accounts and admin accounts when conducting reviews.

INDICATORS OF COMPROMISE TO CONSIDER

NEW ACCOUNT CREATION

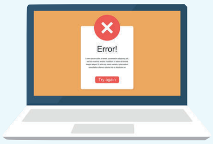
PRIVILEGE ESCALATION

HIGH-PRIVILEGE FEATURE USAGE

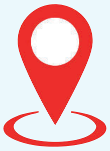
UNUSUAL ACCESS TIMEFRAMES

USERS PERFORMING UNUSUAL TASKS

REPEATED FAILED LOGIN ATTEMPTS



LOGIN LOCATION



ABNORMAL TRAFFIC PATTERNS

APPENDIX A

AUDIT POLICY SETTINGS

Enable Audit Policy Settings with Group Policy. Audit Policy settings are configured in group policy and applied to all computers and servers. *Computer Configuration -> Policies -Windows Settings -> Security Settings -> Advanced Audit Policy Configuration.*

NOTE: *The increased information logged can take up a lot of additional space on workstations and servers. Please set up retentions accordingly.*

	SETTINGS
ACCOUNT LOGON	□ Ensure 'Audit Credential Validation' is set to 'Success and Failure'
ACCOUNT MANAGEMENT	□ Audit 'Application Group Management' is set to 'Success and Failure' □ Audit 'Computer Account Management' is set to 'Success and Failure' □ Audit 'Other Account Management Events' is set to 'Success and Failure' □ Audit 'Security Group Management' is set to 'Success and Failure' □ Audit 'User Account Management' is set to 'Success and Failure'
DETAILED TRACKING	□ Audit 'PNP Activity' is set to 'Success' □ Audit 'Process Creation' is set to 'Success'
LOGON/LOGOFF	□ Audit 'Account Lockout' is set to 'Success and Failure' □ Audit 'Group Membership' is set to 'Success' □ Audit 'Logoff' is set to 'Success' □ Audit 'Logon' is set to 'Success and Failure' □ Audit 'Other Logon/Logoff Events' is set to 'Success and Failure' □ Audit 'Special Logon' is set to 'Success'
OBJECT ACCESS	□ Audit 'Removable Storage' is set to 'Success and Failure'
POLICY CHANGE	□ Audit 'Audit Policy Change' is set to 'Success and Failure' □ Audit 'Authentication Policy Change' is set to 'Success' □ Audit 'Authorization Policy Change' is set to 'Success'
PRIVILEGE USE	□ Audit 'Sensitive Privilege Use' is set to 'Success and Failure'
SYSTEM	□ Audit 'IPsec Driver' is set to 'Success and Failure' □ Audit 'Security State Change' is set to 'Success' □ Audit 'Security System Extension' is set to 'Success and Failure' □ Audit 'System Integrity' is set to 'Success and Failure'

RIC one

TWELVE NEW YORK STATE REGIONAL INFORMATION CENTERS
WORKING AS ONE