Cornwall-Lebanon School District

Vulnerability Management Guideline

Purpose

Cornwall-Lebanon School District's IT assets must be regularly monitored for vulnerabilities in order to identify where there are information security risks. This policy will outline how the vulnerabilities are identified and then managed, including the identification and remediation process behind the different vulnerabilities.

Scope

The Vulnerability Management Policy applies to all information systems and information system components of Cornwall-Lebanon School District. Specifically, it includes:

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, content filters, and other devices that provide dedicated security capabilities.

This policy applies to all IT assets, including hardware, software, and applications, that are owned and operated by Cornwall-Lebanon School District.

Policy Statements

1. Vulnerability assessment and system patching will only be performed by designated individuals. Please see the Vulnerability Mitigation Process document for a list of assigned roles and responsibilities.

2. All IT assets, including all hardware and software components, must be accurately listed in the IT Department asset inventory to aid in the management of vulnerabilities.

3. Vulnerability scanning tools will be used to perform scans of information technology systems to identify information security vulnerabilities. Please see the Vulnerability Mitigation Process document for a schedule of vulnerability scanning.

4. Vulnerabilities will be identified through active monitoring and reviewing of third-party vulnerability sources for any new and unique vulnerabilities that currently exist. Please see the Vulnerability Mitigation Process document for a schedule of third-party vulnerability monitoring.

5. Penetration tests will be conducted by a validated third party in order to identify which vulnerabilities can be exploited by threat actors. Please see the Vulnerability Mitigation Process document for a schedule of third-party penetration tests.

6. Each vulnerability alert and patch release must be checked against existing Cornwall-Lebanon School District systems and services prior to taking any action in order to avoid unnecessary remediation. Read all alerts very carefully – not all patches are related to issues or actual system versions present at Cornwall-Lebanon School District.

7. Each vulnerability will be evaluated and assigned urgency based on the intrinsic qualities of the vulnerability, the criticality of the business systems that it affects, and the sensitivity of the data that can be found on the specific assets.

8. The remediation options that Cornwall-Lebanon School District will be using are: patches, configuration changes, or defense-in-depth controls. The exact solution will be identified based on numerous risk factors including the availability of a patch and the risk accepted by utilizing a different method.

9. If remediation is not implemented, Cornwall-Lebanon School District will accept the risk that comes from leaving the vulnerability open. This will be in accordance with Cornwall-Lebanon School District's risk management framework, and each non-remediated vulnerability must be signed off by management.

10. Backups will be conducted before the implementation of any remediation, in the case that the system needs to be restored. The existing backup schedule can be found the Symantec Backup Exec server.

11. All remediation must be tested prior to full implementation since they may have unforeseen side effects. Reference existing testing procedure documentation. Any exception to testing means that a level of risk is accepted by Cornwall-Lebanon School District. This will be documented and signed off by management.

12. All configuration and inventory documentation must be immediately updated in order to reflect applied remediation.

13. Audits will be performed to ensure that remediation has been applied as required and is functioning as expected.

14. As new systems and assets are added to the system, they are considered in the larger vulnerability management program.