Change and Configuration Management

Tuesday, August 13, 2024 3:18 PM

To ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, the following process for evaluating **Stmt 16: Changes to Information Assets** incorporates the regulatory guidelines on safeguarding member information. This evaluation process aligns with the FFIEC (Federal Financial Institutions Examination Council) guidance on managing risks to the information systems used by financial institutions.

Step 1: Review of Existing Documentation

1. **Collect Existing Policies and Procedures**:
   - Ensure policies and procedures for managing changes to information assets (hardware, software, systems) comply with the institution's **Information Security Program** as mandated by **Appendix A**.
   - **Appendix A to Part 748, Title 12** specifies that institutions must develop, implement, and maintain an information security program to ensure the security and confidentiality of member information, particularly with respect to system changes.
2. **Evaluate Documentation Completeness**:
   - Verify whether the documentation contains elements required by **Appendix A**, such as addressing internal and external threats and vulnerabilities when changes are made to information systems.

Step 2: Evaluate Stmt 16.1 to Stmt 16.2 (CORE Requirements)

1. **Stmt 16.1: Process for Review and Approval of Changes**:
   - **Appendix A** requires that institutions have a comprehensive process to identify and mitigate risks associated with changes to information systems. This should include a formal review and approval process.
   - Ensure that the change management process aligns with the organization's overall risk management practices.
2. **Stmt 16.2: Documentation of Requests and Approvals**:
   - Confirm that documentation processes meet **Appendix A**'s requirement to maintain logs of changes and approvals. Institutions must document approvals to ensure transparency and accountability for system changes that could affect member data security.

Step 3: Evaluate Stmt 16.3 to Stmt 16.15 (CORE+ Requirements)

1. **Stmt 16.3 & 16.4: MFA for Externally-Exposed Applications and Remote Access**:
   - **12 CFR 748.0** emphasizes safeguarding systems and member information. Implementing **MFA** for external applications and remote access enhances compliance with the requirement to control access to systems housing sensitive member data.
   - Test MFA as required under **Appendix A** to ensure that adequate access controls are in place.
2. **Stmt 16.5: Inventory of Authentication and Authorization Systems**:
   - Ensure that the institution maintains an updated inventory of authentication and authorization systems to meet the requirements for managing access controls under **Appendix A**.
3. **Stmt 16.6: Centralized Access Control**:
   - Compliance with **Appendix A** requires institutions to protect member information by ensuring centralized management of access controls.
4. **Stmt 16.7: Role-Based Access Control (RBAC)**:
   - **Appendix A** emphasizes that user access to sensitive systems should be based on roles and responsibilities, thereby limiting access to authorized personnel.
5. **Stmt 16.8: Change Categorization by Severity**:
   - Confirm that the institution's change management policies include categorizing changes by severity to comply with **Appendix A's** guidelines on identifying and managing risks during system changes.
6. **Stmt 16.9: Configuration Management Process**:
   - **Appendix A** requires institutions to establish and maintain baselines for system configurations. This helps to detect unauthorized changes, mitigating risks associated with unauthorized system modifications.
7. **Stmt 16.10: Removal of Nonessential Software**:
   - Verify compliance with **Appendix A**'s directive to eliminate unnecessary software, which could introduce vulnerabilities, as part of the institution's broader effort to secure its information systems.
8. **Stmt 16.11: Standard Builds and Documented Configurations**:
   - Ensure that all systems are built according to documented standards to reduce the risk of misconfigurations that could compromise member information, as specified in **Appendix A**.
9. **Stmt 16.12: Rollback Procedures**:
   - **Appendix A** calls for institutions to implement contingency plans, including rollback procedures, in case changes cause adverse effects on system security or data integrity.
10. **Stmt 16.13: Metrics for Change Management**:

- Institutions should establish metrics to track the effectiveness of the change management process in maintaining information security, aligning with **Appendix A's** focus on monitoring and reporting.

1. **Stmt 16.14: Change Performance Documentation**:
- Documenting the performance of changes ensures that systems continue to operate securely post-change, a key aspect of maintaining an effective information security program under **Appendix A**.
1. **Stmt 16.15: Post-Implementation Review**:
- Ensure that post-implementation reviews are conducted for all changes, as required by **Appendix A**, to verify that changes do not adversely impact the security of member information.

Compliance Summary:

By integrating the requirements of **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, into the **change management process** for information assets, institutions can ensure that all changes are systematically reviewed, documented, and approved while safeguarding member data. This validation process ensures ongoing compliance with regulatory expectations while mitigating risks associated with unauthorized or improper changes to critical systems.

Issues

Friday, September 20, 2024 3:42 PM

1. Lack of Formalized Change Management Process

- **Finding**: The institution does not have a formalized or sufficiently documented change management process.
    - **Impact**: Without a formalized process, changes to critical systems and information assets may not be tracked, reviewed, or approved consistently. This increases the risk of unauthorized changes leading to data breaches or system instability.
    - **Regulatory Reference**: **Appendix A**, Section III, requires a structured approach to managing risks to member information, including through change management.

2. Incomplete or Inadequate Documentation of Change Requests and Approvals

- **Finding**: Change requests, approvals, and documentation are either incomplete or missing.
    - **Impact**: Failure to maintain proper documentation can result in audit findings, as regulators expect clear records of changes that affect the security of member information.
    - **Regulatory Reference**: **Appendix A**, Section III, requires institutions to document their security programs, including controls for systems and networks.

3. Missing or Ineffective Multi-Factor Authentication (MFA) for Externally Exposed Systems

- **Finding**: MFA is not enforced on externally exposed applications or remote access systems, or it is only partially implemented.
    - **Impact**: Without MFA, unauthorized access to sensitive systems is more likely, exposing member information to potential compromise.
    - **Regulatory Reference**: **Appendix A**, Section III(C), requires effective access controls to safeguard information systems from unauthorized access.

4. Failure to Maintain an Up-to-Date Inventory of Authentication and Authorization Systems

- **Finding**: The institution lacks a comprehensive, up-to-date inventory of all authentication and authorization systems.
    - **Impact**: Without an accurate inventory, it is difficult to manage access controls effectively or monitor system changes that could expose security vulnerabilities.
    - **Regulatory Reference**: **Appendix A**, Section III, calls for institutions to establish controls for managing risks to member information, including the maintenance of secure systems.

5. Inadequate Role-Based Access Control (RBAC)

- **Finding**: Access to sensitive information or systems is not limited by role, or the institution's RBAC system is not implemented or maintained correctly.
    - **Impact**: This can result in excessive access, increasing the risk of unauthorized actions and internal fraud.

- **Regulatory Reference**: **Appendix A**, Section III(C), requires institutions to limit access to systems to individuals who need access based on their roles.

6. Failure to Properly Categorize Changes by Severity

- **Finding**: The institution does not categorize system changes by severity, leading to the same approval process for minor and major changes.
  - **Impact**: Critical changes may not receive the scrutiny they require, leading to potential disruptions or security vulnerabilities.
  - **Regulatory Reference**: **Appendix A**, Section III(C), emphasizes the need to monitor and control access to sensitive information systems based on the risks posed by changes.

7. Nonexistent or Outdated Rollback Procedures

- **Finding**: The institution lacks effective rollback procedures for system changes, or the procedures have not been tested recently.
  - **Impact**: In the event of a failed system change, the inability to revert to a previous configuration could result in downtime or data corruption.
  - **Regulatory Reference**: **Appendix A**, Section III(B), emphasizes having contingency plans in place for responding to security incidents or system failures.

8. Nonessential Software or Components Remain on Critical Systems

- **Finding**: The institution has not removed nonessential software, protocols, or services from critical systems.
  - **Impact**: Nonessential software increases the attack surface and can introduce security vulnerabilities that could be exploited by malicious actors.
  - **Regulatory Reference**: **Appendix A**, Section III(C), requires institutions to ensure that all systems housing member information are adequately secured.

9. Inconsistent or Lack of Post-Implementation Testing

- **Finding**: Post-implementation testing is either not performed or inconsistent, leading to potential undetected integration issues or security weaknesses.
  - **Impact**: Without adequate testing, system changes may introduce security vulnerabilities or performance issues.
  - **Regulatory Reference**: **Appendix A**, Section III, requires testing of controls and processes to ensure ongoing protection of member information.

10. Lack of Metrics or Ineffective Use of Change Management Metrics

- **Finding**: The institution does not track or effectively use metrics to monitor the success and impact of change management processes.
  - **Impact**: Without metrics, it becomes difficult to assess whether the change management process is effectively mitigating risks and improving system security.
  - **Regulatory Reference**: **Appendix A**, Section III, recommends continuous monitoring and evaluation of the effectiveness of security measures.

11. Missing or Incomplete Post-Implementation Review

- **Finding**: The institution does not consistently conduct post-implementation reviews of changes, or the reviews are not documented.

- **Impact**: Failing to conduct a post-implementation review increases the risk of overlooking errors, vulnerabilities, or security gaps introduced by changes.
- **Regulatory Reference**: **Appendix A**, Section III, emphasizes the importance of continuous monitoring and reviewing systems after significant changes.

12. Configuration Management Baselines Not Established or Maintained

- **Finding**: Configuration management processes do not establish or maintain baseline configurations for systems.
    - **Impact**: This increases the risk of configuration drift, where systems become misaligned with security standards, potentially exposing them to vulnerabilities.
    - **Regulatory Reference**: **Appendix A**, Section III(C), requires institutions to maintain systems in a manner that protects the confidentiality, integrity, and security of member information.

Remediation

Friday, September 20, 2024 3:44 PM

1. Formalize and Document a Change Management Process

- **Finding**: Lack of a formal change management process.
- **Remediation**:
    - Develop a detailed **Change Management Policy** that defines how changes to systems, applications, and user access are reviewed, approved, implemented, and documented.
    - Define roles and responsibilities for stakeholders, including IT, security, compliance, and management teams.
    - Establish workflows and criteria for emergency, routine, and critical changes, ensuring that each type of change is subject to the appropriate level of review and approval.
    - Provide training to all relevant personnel on the new or updated policy to ensure adherence.

2. Enhance Documentation for Change Requests and Approvals

- **Finding**: Incomplete or missing documentation for change requests and approvals.
- **Remediation**:
    - Implement a centralized **Change Management System (CMS)** or ticketing system that logs all change requests, including approvals, denials, and implementation details.
    - Ensure that the system records the rationale for changes, who authorized the change, and the final outcome.
    - Periodically audit the records to ensure completeness, accuracy, and accessibility.

3. Implement and Enforce Multi-Factor Authentication (MFA)

- **Finding**: Missing or ineffective MFA for externally exposed systems and remote access.
- **Remediation**:
    - Enforce MFA for all externally facing applications, systems, and remote access points (such as VPNs).
    - Deploy MFA solutions (e.g., time-based one-time passwords, hardware tokens, biometric authentication) for privileged accounts and systems handling sensitive member data.
    - Regularly test MFA mechanisms to ensure they are functioning correctly and monitor for any security incidents involving remote access.

4. Maintain an Up-to-Date Inventory of Authentication and Authorization Systems

- **Finding**: Missing or outdated inventory of authentication and authorization systems.
- **Remediation**:
    - Conduct an **inventory audit** of all authentication and authorization systems used in the organization (e.g., Active Directory, SSO, cloud-based services).
    - Implement an automated solution to maintain a real-time, up-to-date inventory of systems, including access controls, configurations, and

responsible personnel.
    - Schedule regular reviews (e.g., quarterly) to ensure the inventory remains accurate and reflective of the current environment.

5. Implement Role-Based Access Control (RBAC)

- **Finding**: Inadequate or improperly implemented RBAC.
- **Remediation**:
    - Define clear **job roles** within the organization, assigning specific access privileges to each role based on operational needs and least privilege principles.
    - Perform a thorough **access review** for each user to ensure that they have access only to the systems and data required for their role.
    - Use **automated tools** to enforce RBAC policies, such as identity and access management (IAM) solutions.

6. Categorize Changes by Severity

- **Finding**: Lack of change severity categorization or inconsistent categorization.
- **Remediation**:
    - Develop a policy to categorize changes based on their potential impact (e.g., minor, moderate, critical).
    - Create a **matrix or severity model** that assigns approval workflows based on the level of risk each category represents.
    - Ensure that changes categorized as high-risk are subject to more stringent review and approval processes (e.g., by senior management or a change advisory board).

7. Establish and Test Rollback Procedures

- **Finding**: Missing or inadequate rollback procedures for system changes.
- **Remediation**:
    - Develop **rollback plans** for each critical system, outlining the steps to revert to a previous stable state if a change fails.
    - Test rollback procedures regularly (e.g., during routine system updates) to ensure they work as expected and that staff are familiar with the process.
    - Document and store rollback procedures in the change management system for easy access during an incident.

8. Remove Nonessential Software, Services, and Protocols

- **Finding**: Nonessential software or services are still present on critical systems.
- **Remediation**:
    - Conduct an audit to identify **nonessential software**, services, or protocols that are no longer needed or used.
    - Establish a process to review and remove unnecessary components from systems, with special attention to services that increase the organization’s attack surface.
    - Regularly schedule **maintenance windows** to assess and remove nonessential software, ensuring that all changes are documented and approved.

9. Implement Post-Implementation Testing and Reviews

- **Finding**: Inconsistent or missing post-implementation testing and reviews.
- **Remediation**:
    - Implement mandatory **post-implementation reviews** for all major

changes to systems or infrastructure.
    - Develop a checklist for testing that includes functional, security, and integration tests to ensure that the changes do not introduce any vulnerabilities or disrupt existing systems.
    - Document the outcomes of these reviews and incorporate any lessons learned into future change management practices.

10. Track Change Management Metrics

- **Finding**: Lack of metrics or ineffective use of metrics to monitor change management performance.
- **Remediation**:
    - Identify and track key **metrics** that measure the effectiveness of the change management process, such as the number of approved changes, changes that resulted in incidents, and time taken to implement changes.
    - Use these metrics to **improve efficiency** and **reduce risks** in the change management process.
    - Regularly report on these metrics to management and use them to guide improvements in the change management process.

11. Remove Expired or Inactive Rules and Objects

- **Finding**: Expired rules, objects, or components are still in place.
- **Remediation**:
    - Conduct regular audits of access rules, permissions, and configurations, identifying any that are no longer relevant (e.g., expired temporary access rules).
    - Implement an automated process for decommissioning expired rules and objects to minimize unnecessary clutter and security risks.

12. Conduct Regular Post-Implementation Reviews

- **Finding**: Inconsistent or missing post-implementation reviews.
- **Remediation**:
    - Require a **post-implementation review** for all changes, especially those affecting critical systems or involving security configurations.
    - Ensure that these reviews assess the impact, success, and any unexpected outcomes of the change.
    - Use the review process to document **lessons learned** and update change management procedures accordingly.

Compliance

Friday, September 20, 2024 3:49 PM

To achieve compliance with **12 CFR 748.0** and **Appendix A to Part 748**, which focus on safeguarding member information through security controls, risk assessments, and incident response, you must establish a structured change and configuration management process. This involves implementing policies, procedures, and controls to protect sensitive information, manage system configurations, and track changes effectively. Below is a comprehensive approach to achieving compliance for **change and configuration management**:

1. Develop a Comprehensive Change Management Policy

- **Action**: Create and document a formal change management policy outlining the procedures for requesting, reviewing, approving, and implementing changes to systems and applications.
- **Compliance Requirement**: Appendix A to Part 748, Title 12 requires a **formal change control process** for ensuring that changes to information systems are documented and managed effectively to minimize risks.
- **Key Considerations**:
  - Define the scope of changes subject to the policy, including software, hardware, network configurations, and user access controls.
  - Establish a Change Advisory Board (CAB) responsible for reviewing and approving changes.
  - Maintain documentation of all changes, approvals, and testing results for audit purposes.

2. Implement Role-Based Access Control (RBAC) for Change Management

- **Action**: Ensure that access to change management tools and configuration settings is restricted based on role and responsibility.
- **Compliance Requirement**: 12 CFR 748.0 requires that access to sensitive systems is restricted and managed effectively.
- **Key Considerations**:
  - Use RBAC to ensure that only authorized personnel can initiate, review, or approve changes.
  - Maintain an up-to-date inventory of user roles and permissions.
  - Periodically review and audit access permissions to ensure compliance.

3. Document and Track All Changes

- **Action**: Use a **ticketing system** or **change management tool** (e.g., ServiceNow, JIRA, or Microsoft SCCM) to document and track all changes, including the reason for the change, the affected systems, and the testing process.
- **Compliance Requirement**: Appendix A to Part 748 requires documenting system changes and ensuring that changes are approved by authorized personnel.
- **Key Considerations**:
  - Ensure that all change requests are documented with details such as the requestor, affected systems, the reason for the change, and testing outcomes.
  - Maintain a log of all approved and rejected changes for audit purposes.
  - Include rollback procedures and contingency plans in the documentation.

4. Enforce Multi-Factor Authentication (MFA) for Externally Exposed Systems

- **Action**: Implement **MFA** for all systems that are accessible externally, such as VPNs, cloud applications, or any remote access points.
- **Compliance Requirement**: Appendix A requires protecting sensitive information through secure access mechanisms, especially for remote access.
- **Key Considerations**:
  - Deploy MFA for all users accessing sensitive systems externally.
  - Ensure that MFA is enforced consistently across the organization, including administrators and privileged users.

5. Conduct Regular Configuration Reviews

- **Action**: Establish a regular review process for system configurations to ensure that configurations remain compliant with security policies and best practices.
- **Compliance Requirement**: Appendix A requires periodic reviews and testing of systems to identify and address vulnerabilities and misconfigurations.
- **Key Considerations**:
  - Develop and maintain baseline configurations for all systems.
  - Schedule regular audits of system configurations (e.g., firewall rules, server settings, and user access permissions).
  - Use automated configuration management tools to track changes and alert security teams of deviations from baseline configurations.

6. Develop and Maintain Configuration Management Procedures

- **Action**: Document and maintain standard procedures for managing system configurations, including how configurations are tested, deployed, and validated.
- **Compliance Requirement**: Appendix A mandates the implementation of security controls, including configuration management, to protect member information.
- **Key Considerations**:
  - Develop a procedure for validating configurations before deployment.
  - Document approved configurations and ensure that all systems adhere to these configurations.
  - Include a process for promptly addressing and correcting misconfigurations.

7. Perform Post-Implementation Reviews and Testing

- **Action**: After implementing changes, perform a post-implementation review to verify that the change achieved the desired outcome without introducing vulnerabilities or operational issues.
- **Compliance Requirement**: Appendix A requires the validation of security controls and testing of changes to ensure they do not compromise system integrity.
- **Key Considerations**:
  - Conduct post-implementation testing to ensure that changes perform as expected.
  - Review system logs and performance metrics after changes are deployed.
  - Document the results of post-implementation testing and report any issues to the Change Advisory Board.

8. Enable Continuous Monitoring for Unauthorized Changes

- **Action**: Implement continuous monitoring tools (e.g., Splunk, SolarWinds, or Nagios) to detect and alert on unauthorized changes to systems, network configurations, and sensitive information.
- **Compliance Requirement**: Appendix A mandates that organizations monitor their systems for unauthorized access and modifications.
- **Key Considerations**:
  - Set up alerts to notify the security team of any unauthorized changes or access attempts.
  - Implement a regular log review process to identify suspicious activity.
  - Ensure that all changes are properly logged and auditable.

9. Test Rollback and Contingency Plans

- **Action**: Establish and regularly test rollback procedures for system changes to ensure that any unintended effects can be mitigated without causing service disruption.
- **Compliance Requirement**: Appendix A emphasizes the importance of incident response and contingency planning.
- **Key Considerations**:
  - Develop and document rollback procedures for critical systems and changes.
  - Conduct tests to verify that rollback procedures are effective and do not cause additional issues.
  - Ensure that rollback procedures are included in change documentation.

10. Audit and Report Compliance with Change Management

- **Action**: Schedule regular audits of the change management process to ensure it complies with 12 CFR 748.0 and Appendix A requirements.
- **Compliance Requirement**: Appendix A requires that security controls, including change management, are periodically audited and reviewed.
- **Key Considerations**:
  - Use internal or external auditors to review the change management process.
  - Create a formal report on change management compliance for the board of directors and other stakeholders.
  - Address any audit findings or gaps through remediation plans.

11. Implement Metrics for Monitoring Change Management Efficiency

- **Action**: Track key metrics to measure the effectiveness of the change management process, such as the number of approved changes, rejected changes, and incidents caused by improper changes.
- **Compliance Requirement**: Appendix A encourages continuous improvement through the measurement and tracking of system security controls.
- **Key Considerations**:
  - Define metrics that can provide insights into the change management process, such as the time to approve changes or the success rate of changes.
  - Use metrics to identify areas for improvement and to optimize the change management process.
  - Report metrics to the Change Advisory Board and other stakeholders.

By following these steps, your organization can ensure that its **change and configuration management process** complies with the requirements of **12 CFR 748.0** and **Appendix A to Part 748**, effectively safeguarding sensitive member information and protecting critical systems.

Tools

Tuesday, August 13, 2024 3:21 PM

1. Change Management and Documentation

- **ServiceNow**
  - *Use Case:* For managing and documenting change requests, approvals, and tracking changes across systems.
  - *Validation:* Ensure that ServiceNow is configured to capture all relevant data for Stmt 16.1 and Stmt 16.2.
- **JIRA**
  - *Use Case:* For documenting requests, approvals, and tracking the status of change requests.
  - *Validation:* Review workflows and documentation procedures for completeness and adherence to policies.
- **Confluence**
  - *Use Case:* For maintaining a centralized repository of change management policies, procedures, and documentation.
  - *Validation:* Check that all documentation is up-to-date and accessible.

2. Multi-Factor Authentication (MFA)

- **Microsoft Azure AD**
  - *Use Case:* Provides MFA for Azure-based applications and services.
  - *Validation:* Verify that MFA is enforced for externally exposed applications and remote access as per Stmt 16.3 and Stmt 16.4.
- **Okta**
  - *Use Case:* MFA solution that integrates with various applications.
  - *Validation:* Review Okta's configuration to ensure MFA is correctly implemented.
- **Duo Security**
  - *Use Case:* MFA solution for securing application access.
  - *Validation:* Test MFA enforcement for remote network access and externally exposed applications.

3. Authentication and Access Control

- **Active Directory (AD)**
  - *Use Case:* For centralized access control and role-based access control (RBAC).
  - *Validation:* Review AD configurations to ensure centralized control and proper role assignments as per Stmt 16.6 and Stmt 16.7.
- **CyberArk**
  - *Use Case:* Privileged access management tool that controls access to critical systems.
  - *Validation:* Verify that privileged access is managed centrally and RBAC is enforced.
- **SailPoint IdentityIQ**
  - *Use Case:* Identity governance tool that ensures compliance and provides access certification.
  - *Validation:* Review identity governance processes to confirm adherence to RBAC principles.
- **Ping Identity**
  - *Use Case:* Identity management tool for centralized access control and authentication.
  - *Validation:* Ensure centralized authentication is configured and operational.

4. Inventory and Configuration Management

- **CMDB (Configuration Management Database)**
  - *Use Case:* Centralized repository to track and manage all IT assets and configurations.
  - *Validation:* Verify that the inventory of authentication and authorization systems is accurate and up-to-date as per Stmt 16.5 and Stmt 16.9.
- **Puppet/Ansible/Chef**
  - *Use Case:* Configuration management tools for automating the deployment and management of systems.
  - *Validation:* Ensure that these tools are used to enforce standard builds and maintain baselines.
- **SolarWinds**
  - *Use Case:* For tracking and managing IT assets, including configurations.
  - *Validation:* Verify that SolarWinds is configured to monitor changes and maintain baselines.
- **Tenable.io**
  - *Use Case:* Vulnerability management tool that also tracks and monitors configurations.
  - *Validation:* Check for nonessential software, protocols, and services as per Stmt 16.10.

5. Security Information and Event Management (SIEM)

- **Splunk**
  - *Use Case:* For monitoring and analyzing security events, including changes in systems and configurations.
  - *Validation:* Verify that Splunk is used to detect and alert on unauthorized or high-severity changes.
- **IBM QRadar**
  - *Use Case:* SIEM tool for real-time monitoring of network and system changes.
  - *Validation:* Ensure QRadar is set up to monitor changes and log all activities.
- **ArcSight**
  - *Use Case:* SIEM tool for centralized logging and event management.
  - *Validation:* Confirm that ArcSight is configured to capture all relevant change management events.

6. Patch Management

- **Microsoft SCCM (System Center Configuration Manager)**
  - *Use Case:* For managing software updates and patches across systems.
  - *Validation:* Review SCCM reports to ensure nonessential software has been removed and standard builds are maintained.
- **Qualys**
  - *Use Case:* Vulnerability and patch management tool.
  - *Validation:* Validate that Qualys is used to identify and apply critical patches.
- **Ivanti Patch Management**
  - *Use Case:* Tool for automating patch deployment and compliance checks.
  - *Validation:* Verify that all systems are up-to-date with required patches and nonessential software is removed.

7. Post-Implementation Review

- **Tableau/Power BI**
  - *Use Case:* For analyzing and visualizing change management metrics.
  - *Validation:* Ensure that identified metrics (Stmt 16.13) are tracked and visualized to monitor the efficiency and success of the change management process.
- **Smartsheet**
  - *Use Case:* For tracking post-implementation reviews and documenting the performance of changes.
  - *Validation:* Review Smartsheet records to ensure that post-implementation reviews (Stmt 16.15) are completed and lessons learned are documented.

- **JIRA (for Metrics)**
    - *Use Case:* For tracking the number of planned vs. unplanned changes and other metrics.
    - *Validation:* Analyze JIRA reports to ensure that metrics are being used to improve the change management process.

8. Rollback Procedures

- **Git/GitHub/GitLab**
    - *Use Case:* Version control tools that allow for rollback of software changes.
    - *Validation:* Review rollback procedures and ensure that they are tested and documented.
- **VMware vSphere**
    - *Use Case:* For taking snapshots of virtual machines before changes, enabling rollback if needed.
    - *Validation:* Confirm that snapshots are used effectively and rollback procedures are in place.
- **Azure DevOps**
    - *Use Case:* For managing the deployment pipeline and rolling back changes if necessary.
    - *Validation:* Test rollback capabilities within the DevOps pipeline to ensure they work as intended.

Resources

Tuesday, August 13, 2024 3:28 PM

https://attack.mitre.org/mitigations/M1028/

https://attack.mitre.org/mitigations/M1054/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

https://github.com/cisagov/ScubaGear?tab=readme-ov-file

https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

https://csf.tools/reference/critical-security-controls/version-7-1/csc-11/

https://csf.tools/reference/critical-security-controls/version-7-1/csc-5/

Policy and Procedure	Review Workstation Security policy and procedure to verify the organization has a formal documented Workstation Security policy and procedure.	Workstation Security policy and procedure	The organization has a formal documented Workstation Security policy and procedure, describing requirements and implementation for workstation hardening, deployment, and patching.
Workstation Image Update	Interview administrator to verify the organization updates any standard images used in deployment no less than monthly.		The organization updates any standard images used in deployment no less than monthly.
Hardening Standards	Interview administrator/Review deployment checklist to verify the organization hardens workstations prior to deployment.	Workstation deployment checklist	The organization hardens workstations prior to deployment using industry security standards, such as NIST, STIGs, or CIS benchmarks.
Patching	Interview administrator to verify that workstations are patched using an automated patching solution at least monthly. Review latest patch status report to verify workstations are appropriately patched	Latest patch status report	Workstations are patched using an automated patching solution at least monthly. Patches are pushed out to a test group for a period of time before being applied to the full production environment. Critical or zero-day patches are applied immediately as needed
Mobile Devices	Interview administrator to confirm mobile devices are controlled and employ encryption	Mobile device agreement	Laptops in use employ full disk encryption. Mobile devices used to access organizational data require device encryption Personal devices are not permitted to access organizational data unless managed by the organization Employees are required to read and acknowledge a Mobile Device agreement detailing their rights and responsibilities
Removable Media	Interview administrator to confirm removable media is restricted.	Removable media GPO screenshot	Removable media is restricted unless explicitly authorized for specific users and/or workstations.
Login Banner	Interview administrator/Review login banner to verify a login banner is in place for monitoring and privacy.	Login banner screenshot	A login banner is in place detailing the organization's monitoring and privacy policy. The login banner requires explicit action for acceptance in order to continue the login process.
Policy and Procedure	Review Server Security policy and procedure to verify the organization has a formal documented Server Security policy and procedure.	Server Security policy and procedure	The organization has a formal documented Server Security policy and procedure, describing requirements and implementation for Server hardening, deployment, and patching.
Server Template Update	Interview administrator to verify the organization scans and updates any virtual templates used in deployment no less than monthly.		The organization scans and updates any virtual templates used in deployment no less than monthly.
Hardening Standards	Interview administrator/Review deployment checklist to verify the organization hardens Servers prior to deployment using industry security standards	Server deployment checklist	The organization hardens Servers prior to deployment using industry security standards, such as NIST, STIGs, or CIS benchmarks.
Patching	Interview administrator to verify that servers are patched using an automated patching solution at least monthly. Review latest patch status report to verify servers are appropriately patched	Latest patch status report	Servers are patched using an automated patching solution at least monthly. Patches are pushed out to a test group for a period of time before being applied to the full production environment. Critical or zero-day patches are applied immediately as needed Core system patches and updates are tested and applied when available.
Remote Administration	Interview administrator to verify remote administration of servers is restricted unless explicitly authorized for specific personnel. Interview and verify methods utilized for remote administration.		Remote administration of servers is restricted unless explicitly authorized for specific personnel. Remote administration is only performed through secure channels.
Hardening Standards	Interview administrator/Review device deployment checklist to verify the organization configures and hardens network devices in accordance with an industry standard checklist.	Device deployment checklist	The organization configures and hardens network devices in accordance with an industry standard checklist. All default passwords are changed and login banners are implemented on configurable network devices.
Policy and Procedure	Review Change Management policy and procedure to confirm the organization has a formal implemented Change Management policy and procedure	Change Management policy and procedure	The organization has a formal implemented Change Management policy and procedure, detailing the requirements and process for requesting, analyzing, approving, testing, applying, and rolling back changes.
Change Process	Interview administrator/Review sample change request to verify the Change process includes: Formal documentation of the request and approval Identification of risks and security requirements Analysis of impact to the organization Change testing Documented rollback process (if required)	Sample change request	

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

From <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a#_Mitigations>

MITIGATIONS

Network Defenders

NSA and CISA recommend network defenders implement the recommendations that follow to mitigate the issues identified in this advisory. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST) as well as with the MITRE ATT&CK Enterprise Mitigations and MITRE D3FEND frameworks.

The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.[24]

Mitigate Default Configurations of Software and Applications

Misconfiguration	Recommendations for Network Defenders
Default configurations of software and applications	• **Modify the default configuration of applications and appliances before deployment** in a production environment [M1013],[D3-ACH]. Refer to hardening guidelines provided by the vendor and related cybersecurity guidance (e.g., DISA's Security Technical Implementation Guides (STIGs) and configuration guides).[25],[26],[27]
Default configurations of software and applications: Default Credentials	• **Change or disable vendor-supplied default usernames and passwords of services, software, and equipment** when installing or commissioning [CPG 2.A]. When resetting passwords, enforce the use of "strong" passwords (i.e., passwords that are more than 15 characters and random [CPG 2.B]) and follow hardening guidelines provided by the vendor, STIGs, NSA, and/or NIST [M1027],[D3-SPP].[25],[26],[28],[29]
Default service permissions and configuration settings: Insecure Active Directory Certificate Services	• **Ensure the secure configuration of ADCS implementations**. Regularly update and patch the controlling infrastructure (e.g., for CVE-2021-36942), employ monitoring and auditing mechanisms, and implement strong access controls to protect the infrastructure. ○ **If not needed, disable web-enrollment in ADCS servers**. See Microsoft: Uninstall-AdcsWebEnrollment (ADCSDeployment) for guidance.[30] ○ If web enrollment is needed on ADCS servers: ▪ **Enable Extended Protection for Authentication (EPA) for Client Authority Web Enrollment**. This is done by choosing the "Required" option. For guidance, see Microsoft: KB5021989: Extended Protection for Authentication.[31] ▪ **Enable "Require SSL"** on the ADCS server. ○ **Disable NTLM** on all ADCS servers. For guidance, see Microsoft: Network security Restrict NTLM in this domain - Windows Security | Microsoft Learn and Network security Restrict NTLM Incoming NTLM traffic - Windows Security.[32],[33] ○ **Disable SAN for UPN Mapping**. For guidance see, Microsoft: How to disable the SAN for UPN mapping - Windows Server. Instead, smart card authentication can use the altSecurityIdentities attribute for explicit mapping of certificates to accounts more securely.[34] • **Review all permissions on the ADCS templates on applicable servers**. Restrict enrollment rights to only those users or groups that require it. Disable the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag from templates to prevent users from supplying and editing sensitive security settings within these templates. Enforce manager approval for requested certificates. Remove FullControl, WriteDacl, and Write property permissions from low-privileged groups, such as domain users, to certificate template objects.
Default service permissions and configuration settings: Insecure legacy protocols/services	• **Determine if LLMNR and NetBIOS are required for essential business operations**. ○ If not required, **disable LLMNR and NetBIOS** in local computer security settings or by group policy.
Default service permissions and configuration settings: Insecure SMB service	• **Require SMB signing** for both SMB client and server on all systems.[25] This should prevent certain adversary-in-the-middle and pass-the-hash techniques. For more information on SMB signing, see Microsoft: Overview of Server Message Block Signing. [35] **Note**: Beginning in Microsoft Windows 11 Insider Preview Build 25381, Windows requires SMB signing for all communications.[36]

Table 1: Recommendations for Network Defenders to Mitigate Default Configurations of Software and Applications

Mitigate Improper Separation of User/Administrator Privilege

Misconfiguration	Recommendations for Network Defenders
Improper separation of user/administrator privilege: • Excessive account privileges, • Elevated service account permissions, and • Non-essential use of elevated accounts	• **Implement authentication, authorization, and accounting (AAA) systems** [M1018] to limit actions users can perform, and review logs of user actions to detect unauthorized use and abuse. Apply least privilege principles to user accounts and groups allowing only the performance of authorized actions. • **Audit user accounts** and remove those that are inactive or unnecessary on a routine basis [CPG 2.D]. Limit the ability for user accounts to create additional accounts. • **Restrict use of privileged accounts to perform general tasks**, such as accessing emails and browsing the Internet [CPG 2.E],[D3-UAP]. See NSA Cybersecurity Information Sheet (CSI) Defend Privileges and Accounts for more information.[37] • **Limit the number of users within the organization with an identity and access management (IAM) role** that has administrator privileges. Strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles, and policies. • **Implement time-based access for privileged accounts**. For example, the just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model) by setting network-wide policy to automatically disable admin accounts at the Active Directory level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe. In cloud environments, just-in-time elevation is also appropriate and may be implemented using per-session federated claims or privileged access management tools. • **Restrict domain users from being in the local administrator group** on multiple systems. • **Run daemonized applications (services) with non-administrator accounts** when possible. • **Only configure service accounts with the permissions necessary for the services they control to operate**. • **Disable unused services and implement ACLs** to protect services.

Table 2: Recommendations for Network Defenders to Mitigate Improper Separation of User/Administrator Privilege

Mitigate Insufficient Internal Network Monitoring

Misconfiguration	Recommendations for Network Defenders
Insufficient internal network monitoring	• **Establish a baseline of applications and services**, and routinely audit their access and use, especially for administrative activity [D3-ANAA]. For instance, administrators should routinely audit the access lists and permissions for of all web applications and services [CPG 2.O],[M1047]. Look for suspicious accounts, investigate them, and remove accounts and credentials, as appropriate, such as accounts of former staff.[39] • **Establish a baseline that represents an organization's normal traffic activity**, network performance, host application activity, and user behavior; investigate any deviations from that baseline [D3-NTCD],[D3-CSPP],[D3-UBA].[40] • **Use auditing tools capable of detecting privilege and service abuse opportunities** on systems within an enterprise and correct them [M1047]. • **Implement a security information and event management (SIEM) system** to provide log aggregation, correlation, querying, visualization, and alerting from network endpoints, logging systems, endpoint and detection response (EDR) systems and intrusion detection systems (IDS) [CPG 2.T],[D3-NTA].

Table 3: Recommendations for Network Defenders to Mitigate Insufficient Internal Network Monitoring

Mitigate Lack of Network Segmentation

Misconfiguration	Recommendations for Network Defenders
Lack of network segmentation	• **Implement next-generation firewalls** to perform deep packet filtering, stateful inspection, and application-level packet inspection [D3-NTF]. Deny or drop improperly formatted traffic that is incongruent with application-specific traffic permitted on the network. This practice limits an actor's ability to abuse allowed application protocols. The practice of allowlisting network applications does not rely on generic ports as filtering criteria, enhancing filtering fidelity. For more information on application-aware defenses, see NSA CSI Segment Networks and Deploy Application-Aware Defenses.[41] • **Engineer network segments to isolate critical systems, functions, and resources** [CPG 2.F],[D3-NI]. Establish physical and logical segmentation controls, such as virtual local area network (VLAN) configurations and properly configured access control lists (ACLs) on infrastructure devices [M1030]. These devices should be baselined and audited to prevent access to potentially sensitive systems and information. Leverage properly configured Demilitarized Zones (DMZs) to reduce service exposure to the Internet.[42],[43],[44] • **Implement separate Virtual Private Cloud (VPC) instances** to isolate essential cloud systems. Where possible, implement Virtual Machines (VM) and Network Function Virtualization (NFV) to enable micro-segmentation of networks in virtualized environments and cloud data centers. Employ secure VM firewall configurations in tandem with macro segmentation.

Table 4: Recommendations for Network Defenders to Mitigate Lack of Network Segmentation

Mitigate Poor Patch Management

Misconfiguration	Recommendations for Network Defenders
Poor patch management: Lack of regular patching	• **Ensure organizations implement and maintain an efficient patch management process** that enforces the use of up-to-date, stable versions of OSs, browsers, and software [M1051],[D3-SU].[45]

	• **Update software regularly by employing patch management** for externally exposed applications, internal enterprise endpoints, and servers. Prioritize patching known exploited vulnerabilities.[2] • **Automate the update process as much as possible** and use vendor-provided updates. Consider using automated patch management tools and software update tools. • Where patching is not possible due to limitations, **segment networks** to limit exposure of the vulnerable system or host.
Poor patch management: Use of unsupported OSs and outdated firmware	• **Evaluate the use of unsupported hardware and software and discontinue use** as soon as possible. If discontinuing is not possible, implement additional network protections to mitigate the risk.[45] • **Patch the Basic Input/Output System (BIOS)** and other firmware to prevent exploitation of known vulnerabilities.

Table 5: Recommendations for Network Defenders to Mitigate Poor Patch Management

Mitigate Bypass of System Access Controls

Misconfiguration	Recommendations for Network Defenders
Bypass of system access controls	• **Limit credential overlap across systems** to prevent credential compromise and reduce a malicious actor's ability to move laterally between systems [M1026],[D3-CH]. Implement a method for monitoring non-standard logon events through host log monitoring [CPG 2.G]. • **Implement an effective and routine patch management process**. Mitigate PtH techniques by applying patch KB2871997 to Windows 7 and newer versions to limit default access of accounts in the local administrator group [M1051],[D3-SU].[46] • **Enable the PtH mitigations to apply User Account Control (UAC) restrictions** to local accounts upon network logon [M1052],[D3-UAP]. • **Deny domain users the ability to be in the local administrator group** on multiple systems [M1018],[D3-UAP]. • **Limit workstation-to-workstation communications**. All workstation communications should occur through a server to prevent lateral movement [M1018],[D3-UAP]. • **Use privileged accounts only on systems requiring those privileges** [M1018],[D3-UAP]. Consider using dedicated Privileged Access Workstations for privileged accounts to better isolate and protect them.[37]

Table 6: Recommendations for Network Defenders to Mitigate Bypass of System Access Controls

Mitigate Weak or Misconfigured MFA Methods

Misconfiguration	Recommendations for Network Defenders

Weak or misconfigured MFA methods: Misconfigured smart cards or tokens	• In Windows environments:
	  ○ **Disable the use of New Technology LAN Manager (NTLM) and other legacy authentication protocols** that are susceptible to PtH due to their use of password hashes [M1032],[D3-MFA]. For guidance, see Microsoft: Network security Restrict NTLM in this domain - Windows Security | Microsoft Learn and Network security Restrict NTLM Incoming NTLM traffic - Windows Security.[32],[33]
	  ○ **Use built-in functionality via Windows Hello for Business or Group Policy Objects (GPOs) to regularly re-randomize password hashes** associated with smartcard-required accounts. Ensure that the hashes are changed at least as often as organizational policy requires passwords to be changed [M1027],[D3-CRO]. Prioritize upgrading any environments that cannot utilize this built-in functionality.
	• As a longer-term effort, **implement cloud-primary authentication solution using modern open standards**. See CISA's Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Architecture for more information.[47] **Note:** this document is part of CISA's Secure Cloud Business Applications (SCuBA) project, which provides guidance for FCEB agencies to secure their cloud business application environments and to protect federal information that is created, accessed, shared, an d stored in those environments. Although tailored to FCEB agencies, the project's guidance is applicable to all organizations.[48]

Weak or misconfigured MFA methods: Lack of phishing-resistant MFA	• **Enforce phishing-resistant MFA universally** for access to sensitive data and on as many other resources and services as possible [CPG 2.H].[3],[49]

Table 7: Recommendations for Network Defenders to Mitigate Weak or Misconfigured MFA Methods

Mitigate Insufficient ACLs on Network Shares and Services

Misconfiguration	Recommendations for Network Defenders
Insufficient ACLs on network shares and services	• **Implement secure configurations for all storage devices** and network shares that grant access to authorized users only. • **Apply the principal of least privilege** to important information resources to reduce risk of unauthorized data access and manipulation. • **Apply restrictive permissions to files and directories**, and prevent adversaries from modifying ACLs [M1022],[D3-LFP]. • **Set restrictive permissions on files and folders containing sensitive private keys** to prevent unintended access [M1022],[D3-LFP]. • **Enable the Windows Group Policy security setting, "Do Not Allow Anonymous Enumeration of Security Account Manager (SAM) Accounts and Shares,"** to limit users who can enumerate network shares.

Table 8: Recommendations for Network Defenders to Mitigate Insufficient ACLs on Network Shares and Services

Mitigate Poor Credential Hygiene

Misconfiguration	Recommendations for Network Defenders
Poor credential hygiene: easily crackable passwords	• **Follow National Institute of Standards and Technologies (NIST) guidelines when creating password policies** to enforce use of "strong" passwords that cannot be cracked [M1027],[D3-SPP].[29] Consider using password managers to generate and store passwords. • **Do not reuse local administrator account passwords across systems**. Ensure that passwords are "strong" and unique [CPG 2.B],[M1027],[D3-SPP]. • **Use "strong" passphrases for private keys** to make cracking resource intensive. Do not store credentials within the registry in Windows systems. Establish an organizati onal policy that prohibits password storage in files. • **Ensure adequate password length (ideally 25+ characters) and complexity requirements for Windows service accounts** and implement passwords with periodic expiration on these accounts [CPG 2.B],[M1027],[D3-SPP]. Use Managed Service Accounts, when possible, to manage service account passwords automatically.
Poor credential hygiene: cleartext password disclosure	• **Implement a review process for files and systems to look for cleartext account credentials**. When credentials are found, remove, change, or encrypt them [D3-FE]. Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, prot ected health information) or credentials are stored. Weigh the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is of sign ificant concern, technical controls, policy, and user training may prevent storage of credentials in improper locations. • **Store hashed passwords using Committee on National Security Systems Policy (CNSSP)-15 and Commercial National Security Algorithm Suite (CNSA) approved algorithms**.[50],[51] • **Consider using group Managed Service Accounts (gMSAs) or third-party software** to implement secure password-storage applications.

Table 9: Recommendations for Network Defenders to Mitigate Poor Credential Hygiene

Mitigate Unrestricted Code Execution

Misconfiguration	Recommendations for Network Defenders
Unrestricted code execution	• **Enable system settings that prevent the ability to run applications downloaded from untrusted sources**.[52] • **Use application control tools that restrict program execution by default, also known as allowlisting** [D3-EAL]. Ensure that the tools examine digital signatures and other key attributes, rather than just relying on filenames, especially since malware often attempts to masquerade as common Operating System (OS) utilities [M1038]. Explicitly allow certain .exe files to run, while blocking all others by default. • **Block or prevent the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode**. Validate driver block rules in audit mode to ensure stability prior to production deployment [D3-OSM]. • **Constrain scripting languages to prevent malicious activities, audit script logs, and restrict scripting languages** that are not used in the environment [D3-SEA]. See joint Cybersecurity Information Sheet: Keeping PowerShell: Security Measures to Use and Embrace.[53] • **Use read-only containers and minimal images**, when possible, to prevent the running of commands. • **Regularly analyze border and host-level protections, including spam-filtering capabilities**, to ensure their continued effectiveness in blocking the delivery and execution of malware [D3-MA]. Assess whether HTML Application (HTA) files are used for business purposes in your environment; if HTAs are not used, remap the default program for opening them from mshta.exe to notepad.exe.

Table 10: Recommendations for Network Defenders to Mitigate Unrestricted Code Execution

Software Manufacturers

NSA and CISA recommend software manufacturers implement the recommendations in Table 11 to reduce the prevalence of misconfigurations identified in this advisory. These mitigations align with tactics provided in joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. NSA and CISA strongly encourage software manufacturers apply these recommendations to ensure their products are secure "out of the box" and do not require customers to spend additional resources making configuration changes, performing monitoring, and conducting routine updates to keep their systems secure.[1]

Misconfiguration	Recommendations for Software Manufacturers
Default configurations of software and applications	• **Embed security controls into product architecture from the start of development and throughout the entire SDLC** by following best practices in NIST's Secure Software Development Framework (SSDF), SP 800-218.[54]

	• **Provide software with security features enabled "out of the box" and accompanied with "loosening" guides** instead of hardening guides. "Loosening" guides should explain the business risk of decisions in plain, understandable language.
Default configurations of software and applications: Default credentials	• **Eliminate default passwords**: Do not provide software with default passwords that are universally shared. To eliminate default passwords, require administrators to set a "strong" password [CPG 2.B] during installation and configuration.
Default configurations of software and applications: Default service permissions and configuration settings	• **Consider the user experience consequences of security settings**: Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.
Improper separation of user/administrator privilege: • Excessive account privileges, • Elevated service account permissions, and • Non-essential use of elevated accounts	• **Design products so that the compromise of a single security control does not result in compromise of the entire system**. For example, ensuring that user privileges are narrowly provisioned by default and ACLs are employed can reduce the impact of a compromised account. Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application. • **Automatically generate reports for:** ○ **Administrators of inactive accounts.** Prompt administrators to set a maximum inactive time and automatically suspend accounts that exceed that threshold. ○ **Administrators of accounts with administrator privileges** and suggest ways to reduce privilege sprawl. • **Automatically alert administrators of infrequently used services** and provide recommendations for disabling them or implementing ACLs.
Insufficient internal network monitoring	• **Provide high-quality audit logs to customers at no extra charge**. Audit logs are crucial for detecting and escalating potential security incidents. They are also crucial during an investigation of a suspected or confirmed security incident. Consider best practices such as providing easy integration with a security information and event management (SIEM) system with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.
Lack of network segmentation	• **Ensure products are compatible with and tested in segmented network environments**.
Poor patch management: Lack of regular patching	• **Take steps to eliminate entire classes of vulnerabilities by embedding security controls into product architecture from the start of development and throughout the SDLC by following best practices in NIST's SSDF**, SP 800-218.[54] Pay special attention to: ○ **Following secure coding practices** [SSDF PW 5.1]. Use memory-safe programming languages where possible, parametrized queries, and web template languages. ○ **Conducting code reviews** [SSDF PW 7.2, RV 1.2] against peer coding standards, checking for backdoors, malicious content, and logic flaws. ○ **Testing code to identify vulnerabilities** and verify compliance with security requirements [SSDF PW 8.2]. • **Ensure that published CVEs include root cause or common weakness enumeration (CWE)** to enable industry-wide analysis of software security design flaws.
Poor patch management: Use of unsupported operating OSs and outdated firmware	• **Communicate the business risk of using unsupported OSs and firmware** in plain, understandable language.
Bypass of system access controls	• **Provide sufficient detail in audit records to detect bypass of system controls** and queries to monitor audit logs for traces of such suspicious activity (e.g., for when an essential step of an authentication or authorization flow is missing).
Weak or Misconfigured MFA Methods: Misconfigured Smart Cards or Tokens	• **Fully support MFA for all users**, making MFA the default rather than an opt-in feature. Utilize threat modeling for authentication assertions and alternate credentials to examine how they could be abused to bypass MFA requirements.
Weak or Misconfigured MFA Methods: Lack of phishing-resistant MFA	• **Mandate MFA, ideally phishing-resistant, for privileged users** and make MFA a default rather than an opt-in feature.[3]
Insufficient ACL on network shares and services	• **Enforce use of ACLs** with default ACLs only allowing the minimum access needed, along with easy-to-use tools to regularly audit and adjust ACLs to the minimum access needed.
Poor credential hygiene: easily crackable passwords	• **Allow administrators to configure a password policy consistent with NIST's guidelines**—do not require counterproductive restrictions such as enforcing character types or the periodic rotation of passwords.[29] • **Allow users to use password managers** to effortlessly generate and use secure, random passwords within products.
Poor credential hygiene: cleartext password disclosure	• **Salt and hash passwords using a secure hashing algorithm** with high computational cost to make brute force cracking more difficult.
Unrestricted code execution	• **Support execution controls** within operating systems and applications "out of the box" by default at no extra charge for all customers, to limit malicious actors' ability to abuse functionality or launch unusual applications without administrator or informed user approval.

Table 11: Recommendations for Software Manufacturers to Mitigate Identified Misconfigurations

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, NSA and CISA recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. NSA and CISA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 12–Table 21).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and NSA recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

LEARN FROM HISTORY

The misconfigurations described above are all too common in assessments and the techniques listed are standard ones leveraged by multiple malicious actors, resulting in numerous real network compromises. Learn from the weaknesses of others and implement the mitigations above properly to protect the network, its sensitive information, and critical missions.

From <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a#_Mitigations>

1. Default Configurations of Software and Applications

- **Misconfiguration**: Use of default configurations can leave systems vulnerable to exploitation.
- **Compliance Steps**:
  - Review and modify default configurations following **vendor guidelines** (e.g., **STIGs**).
  - Disable or change **default credentials** immediately upon installation.
  - Implement **password policies** that require complex, strong passwords (e.g., 15+ characters) and **multi-factor authentication (MFA)** for critical systems.
  - Regularly audit configurations of software to ensure that they meet both vendor and regulatory security standards.
  - For **Active Directory Certificate Services (ADCS)**, disable unnecessary services like web enrollment and enforce strong access controls as recommended.
- **Remediation**:
  - Apply **patches** regularly and follow vendor-specific hardening guides for applications.
  - Audit all default configurations and adjust them based on risk assessments.

2. Improper Separation of User/Administrator Privileges

- **Misconfiguration**: Excessive or improper account privileges.
- **Compliance Steps**:
  - Implement **least privilege** principles and review permissions regularly.
  - Use **role-based access control (RBAC)** to ensure that administrative roles are properly scoped and defined.
  - Review and remove any **inactive or unnecessary user accounts** as part of regular audits.
  - Limit **privileged accounts** from performing general tasks (e.g., browsing the internet).
  - Use **time-based access control** to enable privileged access only when needed, such as **just-in-time access** for admin roles.
- **Remediation**:
  - Conduct regular **access reviews** and disable accounts with excessive or unnecessary privileges.
  - Implement a **privileged access management (PAM)** solution to control and monitor the use of elevated privileges.

3. Insufficient Internal Network Monitoring

- **Misconfiguration**: Lack of visibility into internal network activity.
- **Compliance Steps**:
  - Implement **Security Information and Event Management (SIEM)** systems for log aggregation and monitoring.
  - Establish and regularly update a **baseline of normal network activity**, ensuring that any deviations from the baseline are promptly investigated.
  - Implement **endpoint detection and response (EDR)** solutions to monitor system behavior and detect malicious activity.
  - Ensure auditing capabilities are in place to detect **privilege abuse** or unauthorized access.
- **Remediation**:
  - Regularly audit access to critical systems and ensure that logging is enabled for all sensitive resources.
  - Use **automated tools** to monitor network traffic and detect anomalies.

4. Lack of Network Segmentation

- **Misconfiguration**: Flat networks that lack proper segmentation.
- **Compliance Steps**:
  - Implement **network segmentation** using **virtual local area networks (VLANs)**, **firewalls**, and **demilitarized zones (DMZs)** to isolate critical systems from general network traffic.
  - Use **next-generation firewalls** to perform deep packet inspection and control traffic based on application awareness, not just ports.
  - Apply **micro-segmentation** in virtual environments to isolate systems and limit lateral movement.
- **Remediation**:
  - Audit network configurations to identify systems or devices that are not properly segmented.
  - Implement segmentation policies and use access control lists (ACLs) to restrict traffic between segments.

5. Poor Patch Management

- **Misconfiguration**: Delays or failure to patch software and hardware.
- **Compliance Steps**:
  - Develop and implement an **automated patch management process** for operating systems, browsers, and software.
  - Prioritize patching of known **exploited vulnerabilities** and use tools to track and manage patch deployments.
  - For systems where patching is not feasible (e.g., legacy systems), segment the network to limit exposure and apply additional compensating controls.
- **Remediation**:
  - Set up **automated patching** for all systems and prioritize patching critical vulnerabilities.
  - Regularly review patch status and ensure unsupported software or hardware is replaced or appropriately isolated.

6. Bypass of System Access Controls

- **Misconfiguration**: Weak or bypassed system access controls.
- **Compliance Steps**:
  - Implement **strong password policies** across all systems, ensuring passwords are complex and unique across different systems.
  - Disable **legacy authentication protocols** (e.g., NTLM) that can be exploited to bypass access controls.
  - Limit **lateral movement** by restricting workstation-to-workstation communication and enforcing the principle of least privilege.
- **Remediation**:
  - Audit systems to identify and disable **unused or legacy authentication methods**.
  - Implement **multi-factor authentication (MFA)** for privileged access to critical systems.

7. Weak or Misconfigured MFA Methods

- **Misconfiguration**: Inadequate MFA configuration, such as weak or phishing-vulnerable MFA methods.
- **Compliance Steps**:
  - Implement **phishing-resistant MFA**, such as **FIDO2** or **smartcards**, for privileged accounts and critical resources.
  - Regularly review MFA configurations to ensure they meet security standards, and test for potential bypass vulnerabilities.
  - Disable **legacy authentication protocols** (e.g., NTLM) that do not support MFA.
- **Remediation**:
  - Enforce MFA for all users accessing critical systems and external applications, ensuring robust methods such as **hardware tokens** are used where possible.
  - Regularly audit MFA configurations and test their effectiveness.

8. Insufficient ACLs on Network Shares and Services

- **Misconfiguration**: Weak access control lists (ACLs) allowing unauthorized access.
- **Compliance Steps**:
  - Apply **least privilege** principles to all network shares and services, ensuring ACLs restrict access to authorized users only.
  - Regularly audit ACLs on critical resources, such as file servers and databases, to ensure they are correctly configured.
  - Implement **encryption** on sensitive files and directories to prevent unauthorized access.
- **Remediation**:
  - Review ACLs on all shared resources and tighten permissions as needed.
  - Implement **encryption and auditing** to monitor access to sensitive data and resources.

9. Poor Credential Hygiene

- **Misconfiguration**: Use of easily crackable or weak passwords and improper credential management.
- **Compliance Steps**:
  - Follow **NIST password guidelines** to enforce the use of strong, unique passwords.
  - Implement a **password manager** to store and manage credentials securely.
  - Ensure **service accounts** and **administrator accounts** use long, complex passphrases and rotate passwords regularly.
- **Remediation**:
  - Audit passwords to ensure they meet complexity requirements, and enforce regular password changes where needed.
  - Use tools like **LAPS** (Local Administrator Password Solution) for managing local account passwords.

10. Unrestricted Code Execution

- **Misconfiguration**: Allowing unrestricted execution of potentially malicious code.
- **Compliance Steps**:
  - Implement **application control policies** (e.g., allowlisting) to restrict the execution of untrusted software.
  - Disable unnecessary scripting environments and review script logs to identify misuse.
- **Remediation**:
  - Audit systems for unapproved software and restrict execution to trusted applications using tools like **Microsoft AppLocker** or **Windows Defender Application Control (WDAC)**.

Next Steps for Compliance

1. **Perform a full audit** of the current configuration for all critical systems and services against the recommendations and required controls.
2. **Deploy automated monitoring tools** (SIEM, EDR) to detect potential misconfigurations in real time.
3. **Regularly test configurations**, patches, and access controls through internal and external penetration testing.
4. **Document changes** and enforce strict change control processes to ensure that all security-related configurations are approved and reviewed.
5. **Conduct regular employee training** on security best practices, including credential management, network segmentation, and access control policies.

Browser Configuration

Wednesday, September 18, 2024 11:54 AM

Here's a detailed step-by-step guide for setting up Group Policy Objects (GPOs) to manage browser security settings for Internet Explorer/Edge, Chrome, and Firefox in an Active Directory environment:

1. Prepare the Environment

- **Ensure Domain Controllers Are Running**: Verify that your domain controllers are active and Group Policy Management is accessible.
- **Admin Rights**: You must have administrative privileges to create and manage GPOs within the domain.

2. Download and Install Administrative Templates

- **For Microsoft Edge/Internet Explorer**: These templates are already included with Windows.
- **For Chrome**:
  - Visit the official Chrome Enterprise website to download the `.admx` and `.adml` files.
  - Install them by copying the `.admx` files to `C:\Windows\PolicyDefinitions` and the `.adml` files to `C:\Windows\PolicyDefinitions\<language>` (e.g., `en-US`).
- **For Firefox**:
  - Download the Firefox administrative templates from Mozilla's GitHub repository.
  - Install in the same way as Chrome templates.

3. Create a Group Policy Object (GPO)

1. **Open Group Policy Management**:
   - Open the Group Policy Management Console (GPMC) via `gpedit.msc` or by searching from the Start Menu.
2. **Create a New GPO**:
   - Right-click the Organizational Unit (OU) or domain where you want to apply the GPO and select **Create a GPO in this domain, and Link it here**.
   - Name the GPO appropriately, such as "Browser Hardening".

4. Configure Security Settings for Browsers

4.1 Internet Explorer/Edge:

- Navigate to **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Microsoft Edge** or **Internet Explorer**.
- Configure the following settings:
  - Disable **JavaScript**.
  - Enable **Enhanced Protected Mode**.
  - Set corporate homepages.
  - Manage add-ons (disable unapproved add-ons).
  - Configure pop-up blocking.
  - Block websites or URLs (using Content Advisor or SafeSearch settings).

4.2 Google Chrome:

- Navigate to **Computer Configuration** → **Administrative Templates** → **Google** → **Google Chrome**.
- Configure settings like:
  - Disable **Incognito Mode**.
  - Enforce **Safe Browsing** to protect against malware.
  - Restrict **extensions** (allow only whitelisted extensions).
  - Manage **cookies** settings.
  - Set corporate **homepage URLs**.
  - Disable auto-fill and password saving.

4.3 Mozilla Firefox:

- Navigate to **Computer Configuration** → **Administrative Templates** → **Mozilla** → **Firefox**.
- Set policies such as:
  - Configure **security zones**.
  - Restrict access to certain browser features (like telemetry).
  - Enforce **Safe Browsing**.
  - Manage add-ons (disable all unapproved add-ons).
  - Set **proxy settings**.

5. Testing and Validation

- **Test the GPO on a Small OU or Test Group**: Before rolling out to production, apply the GPO to a test Organizational Unit (OU) or a group of users.
- **Force Policy Update**: On client machines, use `gpupdate /force` to apply the GPO immediately.
- **Verify Settings**:
  - For Chrome, check the settings by navigating to `chrome://policy/`.
  - For Firefox, use `about:policies`.
  - For Edge, verify settings under **Edge settings**.
- **Review**: Ensure that all security configurations are properly applied and functioning as expected.

6. Deploy the GPO

- Once the GPO has been tested and validated:
  - Link the GPO to the appropriate **OU or domain level** for production deployment.
  - **Monitor Deployment**: Use `gpresult /r` or the Group Policy Results tool to ensure all settings are applied correctly to users and computers.

7. Ongoing Maintenance

- **Review and Update the GPO Regularly**: Keep the GPO updated to account for new browser features and security threats.
- **Document Changes**: Maintain detailed documentation of the changes made to the GPO, including the rationale for the changes.
- **User Training**: Educate users on why certain browser functionalities (like Incognito Mode or unauthorized extensions) are disabled for secu rity reasons.
- **Auditing**: Regularly audit browser settings on client machines to ensure compliance and detect potential policy violations.

Additional Tips:

- **Keep Browsers Updated**: Ensure that all browsers are updated to their latest versions to minimize security vulnerabilities.

- **Implement Logging**: Enable logging for any changes to GPOs and monitor logs for any unauthorized changes.
- **Periodic Security Reviews**: Regularly review browser settings as part of your organization's security audits.

This method ensures robust security controls over browsers, minimizing risks from unapproved configurations or unsafe browsing practices.

1. Enforce HTTPS
- **Enforce HTTPS** across your organization by using tools like HTTP Strict Transport Security (HSTS) on your web servers. This prevents browsers from accessing insecure (HTTP) sites and mitigates man-in-the-middle attacks.
- **Enable Secure DNS** (DNS over HTTPS) for browsers that support it (e.g., Chrome, Firefox). This encrypts DNS queries, preventing them from being exposed to third parties.

2. Disable Browser Caching for Sensitive Information
- Configure browsers not to cache sensitive data, such as login forms or payment details. This prevents the retrieval of sensitive information from the browser's cache.
- You can implement this using headers like `Cache-Control: no-store` on web applications handling sensitive information.

3. Block Third-Party Cookies
- Block or restrict third-party cookies by configuring browsers to only allow first-party cookies. This prevents cross-site tracking and mitigates privacy risks.
- Enable **same-site cookie policies** for web applications to prevent cross-site request forgery (CSRF) attacks.

4. Use Content Security Policy (CSP)
- Apply **Content Security Policies (CSP)** to your organization's web applications. CSP helps prevent attacks like cross-site scripting (XSS) by controlling what resources (scripts, images, etc.) can be loaded.
- Regularly audit and adjust your CSP for any new features or threats to ensure that your web apps remain secure.

5. Disable Browser Plugins and Extensions
- **Disable or restrict the use of unnecessary browser plugins and extensions**. Many browser extensions can introduce vulnerabilities or act as spyware.
- Whitelist only approved extensions and block the installation of unauthorized plugins through Group Policy or browser management tools.

6. Implement Strict JavaScript Controls
- Disable or limit **JavaScript execution** on websites unless absolutely necessary. JavaScript can be a vector for XSS or malware attacks.
- Use tools like **NoScript** or configure the browser to only allow JavaScript execution from trusted domains.

7. Enable Anti-Phishing and Anti-Malware Features
- Ensure that the built-in **anti-phishing** and **anti-malware** features in browsers (e.g., Safe Browsing in Chrome and Firefox) are enabled. These features help detect and block malicious websites before they can harm the user.
- Regularly review logs for phishing attempts or malware alerts.

8. Sandbox Browsers for High-Risk Users
- For high-risk users or roles (e.g., executives, IT admins), consider running browsers inside a **sandbox environment**. This isolates the browser from the rest of the operating system, reducing the impact of potential compromises.
- Use **sandboxing tools** like Microsoft's **Windows Sandbox** or other third-party sandboxing solutions.

9. Disable Autofill Features
- Disable browser **autofill** for forms that store personal information (such as usernames, passwords, or credit card numbers). Autofill can expose sensitive data to unauthorized access, especially in shared systems.
- Use dedicated password management tools for storing credentials instead of relying on browser autofill.

10. Regularly Clear Browser Data
- Ensure that **browsing history, cookies, and cached data** are cleared regularly, either through user behavior or automatically via Group Policy or browser settings.
- For high-security environments, consider configuring browsers to **clear data** on exit.

11. Use Private Browsing/InPrivate Mode for Sensitive Work
- Encourage users to use **private browsing** or **incognito mode** when accessing sensitive information or using shared systems. This prevents the browser from storing session data, browsing history, or cookies.
- Restrict private browsing for certain use cases if necessary (i.e., for work-related activities only).

12. Disable WebRTC
- **WebRTC (Web Real-Time Communication)** can expose local IP addresses, even when using VPNs, which poses a privacy risk. Disable WebRTC if your organization doesn't need it.
- In Chrome and Firefox, you can disable WebRTC through browser settings or use extensions that block WebRTC leaks.

13. Use Browser Isolation for External Websites
- Implement **browser isolation** technology for users who frequently visit untrusted or external websites. This isolates the web browsing session in a remote container, preventing any potential threats from reaching the endpoint.

14. Enforce Certificate Validation
- Configure browsers to **strictly enforce SSL/TLS certificate validation** to prevent access to sites with expired, self-signed, or misconfigured certificates.
- Implement **Certificate Pinning** to ensure browsers only trust certificates from predefined sources.

15. Monitor Browser Usage with Security Tools
- Use tools like **Cloud Access Security Brokers (CASBs)** or other monitoring systems to track and control browser usage, especially for cloud services or web applications.
- Implement **real-time monitoring** of browser sessions and usage patterns for detecting anomalies.

16. Enforce Download Restrictions
- Enforce download restrictions via browser settings or Group Policy to prevent users from downloading unsafe file types or software.
- Use browser **sandboxing or Virtual Machines (VMs)** to allow users to safely interact with potentially risky files.

17. Disable Browser Debugging Tools
- Disable developer tools (F12) for non-technical staff to prevent users from accessing sensitive information or accidentally making changes to web applications.
- Use Group Policy or third-party tools to restrict access to these features.

Comments

Thursday, September 26, 2024 3:26 PM

. Comprehensive Change Management Policy

- **Finding**: "The credit union has developed and documented a comprehensive change management policy that clearly outlines the process for requesting, reviewing, approving, and implementing system changes. The policy includes oversight by a Change Advisory Board (CAB), ensuring all changes are carefully evaluated for security risks before implementation, in compliance with Appendix A."

2. Role-Based Access Control (RBAC) for Change Management

- **Finding**: "Access to change management tools and configuration settings is governed by Role-Based Access Control (RBAC), ensuring that only authorized personnel can initiate, review, or approve changes. Access roles are regularly audited to ensure they are aligned with current job responsibilities, in compliance with 12 CFR 748.0."

3. Documentation and Tracking of All Changes

- **Finding**: "All changes to systems, software, and configurations are tracked through a formal ticketing system (e.g., ServiceNow), providing detailed records of change requests, approvals, testing results, and implementation steps. This documentation supports audit requirements under Appendix A and provides a clear trail of all system modifications."

4. Multi-Factor Authentication (MFA) for Externally Exposed Systems

- **Finding**: "Multi-Factor Authentication (MFA) has been implemented for all externally accessible systems, including remote access points and cloud applications. MFA ensures that all users, including administrators, must pass a second layer of authentication, reducing the risk of unauthorized access, in line with Appendix A's requirements for secure remote access."

5. Regular Configuration Reviews

- **Finding**: "The credit union performs regular reviews of system configurations, including firewall rules, server settings, and user access permissions. Automated tools are used to track and monitor configuration changes, and alerts are set for deviations from baseline configurations, ensuring continued compliance with security policies and Appendix A requirements."

6. Configuration Management Procedures

- **Finding**: "Standard procedures for managing system configurations are documented and followed, including thorough testing, validation, and approval before deployment. These procedures ensure that system configurations are secure and consistent with approved settings, as mandated by Appendix A."

7. Post-Implementation Reviews and Testing

- **Finding**: "After changes are implemented, post-implementation reviews and tests are conducted to verify that changes achieve the intended outcome without introducing vulnerabilities. The results of these reviews are documented and shared with the Change Advisory Board, ensuring ongoing compliance with Appendix A's requirement to validate security controls."

8. Continuous Monitoring for Unauthorized Changes

- **Finding**: "Continuous monitoring tools, such as Splunk and SolarWinds, are in place to detect and alert the security team of any unauthorized changes to system configurations or sensitive data. Regular log reviews and automated alerts provide an additional layer of security and compliance with Appendix A's monitoring requirements."

9. Tested Rollback and Contingency Plans

- **Finding**: "Rollback and contingency plans are established for all critical system changes, and these procedures are regularly tested to ensure they can be executed effectively if a change introduces issues. These tests confirm that rollback plans are well-documented and capable of minimizing disruptions, in alignment with Appendix A's focus on incident response and risk mitigation."

10. Auditing and Reporting of Change Management Compliance

- **Finding**: "Regular audits are conducted to evaluate the effectiveness and compliance of the change management process with 12 CFR 748.0 and Appendix A. Audit reports are reviewed by internal stakeholders and the board of directors, ensuring that any identified gaps are addressed promptly through a structured remediation process."

11. Metrics for Monitoring Change Management Efficiency

- **Finding**: "Key performance metrics, such as the number of changes approved, rejected, or requiring rollback, are tracked to assess the effectiveness of the change management process. These metrics are reviewed regularly by the Change Advisory Board to identify areas for improvement and to ensure continuous compliance with Appendix A."

General Positive Findings Across All Areas

- **Robust Change Management Documentation**: "All changes to critical systems are thoroughly documented, with records maintained for approvals, testing outcomes, and rollback procedures. This ensures full compliance with regulatory requirements for documenting and managing changes."
- **Continuous Improvement**: "The credit union employs metrics and regular reviews of the change management process to continuously improve system security. Any issues identified through post-implementation reviews or audits are promptly addressed, ensuring alignment with 12 CFR 748.0 and Appendix A."
- **Security Controls and Risk Management**: "The change and configuration management processes are designed to minimize the risks of unauthorized changes, data breaches, or system misconfigurations. Regular configuration reviews, post-implementation testing, and continuous monitoring ensure that systems remain secure and compliant with regulatory requirements."

Questions

Thursday, October 10, 2024 3:54 PM

1. Develop a Comprehensive Change Management Policy

- **Q1.1**: Is there a formal, documented change management policy in place that covers procedures for requesting, reviewing, approving, and implementing changes to systems and applications?
- **Q1.2**: Does the policy clearly define the scope of changes, including software, hardware, network configurations, and user access controls?
- **Q1.3**: Is a Change Advisory Board (CAB) established, and is it responsible for reviewing and approving all changes?
- **Q1.4**: Are all change requests, approvals, and testing results documented and maintained for audit purposes?
- **Q1.5**: Is the change management policy reviewed and updated periodically to reflect regulatory and business requirements?

2. Implement Role-Based Access Control (RBAC) for Change Management

- **Q2.1**: Is access to change management tools and configuration settings restricted based on roles and responsibilities?
- **Q2.2**: Are role-based access controls (RBAC) implemented to ensure that only authorized personnel can initiate, review, or approve changes?
- **Q2.3**: Is there an up-to-date inventory of user roles, responsibilities, and permissions related to change management activities?
- **Q2.4**: Are periodic audits conducted to review and validate access permissions and ensure compliance with the RBAC policy?

3. Document and Track All Changes

- **Q3.1**: Is a ticketing system or change management tool (e.g., ServiceNow, JIRA, or Microsoft SCCM) used to document and track all changes, including the reason for the change, the affected systems, and the testing process?
- **Q3.2**: Does the change documentation include detailed information such as the requestor, the impact analysis, testing outcomes, and rollback plans?
- **Q3.3**: Are logs of all approved and rejected changes maintained for audit and compliance review?
- **Q3.4**: Are rollback procedures and contingency plans documented and included as part of the change request process?

4. Enforce Multi-Factor Authentication (MFA) for Externally Exposed Systems

- **Q4.1**: Is MFA implemented for all systems that are accessible externally, including VPNs, cloud applications, and remote access points?
- **Q4.2**: Is MFA enforced consistently for all users accessing sensitive systems externally, including administrators and privileged users?
- **Q4.3**: Are regular audits conducted to ensure that MFA is properly configured and enforced across the organization?

5. Conduct Regular Configuration Reviews

- **Q5.1**: Is there a process in place for regularly reviewing system configurations to ensure they comply with security policies and best practices?

- **Q5.2**: Are baseline configurations maintained for all systems, including details like software versions, patch levels, and network settings?
- **Q5.3**: Are regular audits conducted to review system configurations such as firewall rules, server settings, and user access permissions?
- **Q5.4**: Are automated tools used to track configuration changes and alert the security team of any deviations from baseline configurations?

6. Develop and Maintain Configuration Management Procedures

- **Q6.1**: Are standard procedures for managing system configurations documented and maintained, including steps for testing, deploying, and validating configurations?
- **Q6.2**: Are configurations validated before deployment to ensure compliance with security and operational standards?
- **Q6.3**: Are approved configurations documented, and are all systems configured according to these approved standards?
- **Q6.4**: Is there a process for promptly addressing and correcting misconfigurations, and is it documented in the configuration management procedures?

7. Perform Post-Implementation Reviews and Testing

- **Q7.1**: Are post-implementation reviews performed to verify that changes achieved the desired outcome without introducing new vulnerabilities or operational issues?
- **Q7.2**: Are post-implementation tests conducted to validate the effectiveness of changes made to the systems?
- **Q7.3**: Are system logs and performance metrics reviewed after implementing changes to identify any potential issues?
- **Q7.4**: Are the results of post-implementation testing documented, and are any issues reported to the CAB for further review?

8. Enable Continuous Monitoring for Unauthorized Changes

- **Q8.1**: Are continuous monitoring tools (e.g., Splunk, SolarWinds, or Nagios) implemented to detect and alert the security team of unauthorized changes to systems and configurations?
- **Q8.2**: Are alerts configured to notify the security team of any unauthorized changes or access attempts in real-time?
- **Q8.3**: Is there a regular log review process to identify and investigate suspicious activities?
- **Q8.4**: Are all changes properly logged, and are these logs available for audit purposes?

9. Test Rollback and Contingency Plans

- **Q9.1**: Are rollback procedures established for system changes, and are they documented for critical systems and changes?
- **Q9.2**: Are tests conducted to verify the effectiveness of rollback procedures and ensure they do not introduce additional issues?
- **Q9.3**: Are rollback procedures included in change documentation and reviewed regularly for accuracy?
- **Q9.4**: Are contingency plans tested to verify their effectiveness in minimizing service disruptions?

10. Audit and Report Compliance with Change Management

- **Q10.1**: Are regular audits conducted to review the change management process for compliance with 12 CFR 748.0 and Appendix A requirements?
- **Q10.2**: Is there a formal report on change management compliance prepared for

the board of directors and other stakeholders?
- **Q10.3**: Are audit findings or gaps addressed through documented remediation plans?
- **Q10.4**: Is the change management process periodically reviewed and updated based on audit results and regulatory updates?

11. Implement Metrics for Monitoring Change Management Efficiency

- **Q11.1**: Are key metrics defined to measure the effectiveness of the change management process, such as the number of approved changes, rejected changes, and incidents caused by improper changes?
- **Q11.2**: Are metrics such as time to approve changes or success rates tracked and analyzed to identify areas for improvement?
- **Q11.3**: Are the results of these metrics reported to the CAB and other relevant stakeholders?
- **Q11.4**: Are metrics used to optimize the change management process and align it with organizational goals and regulatory requirements?

Answers

Thursday, October 10, 2024 3:55 PM

1. Develop a Comprehensive Change Management Policy

- **Q1.1**: Is there a formal, documented change management policy in place?
    - **Positive**: "Yes, a comprehensive change management policy is documented, outlining all procedures for requesting, reviewing, approving, and implementing changes."
    - **Negative**: "No, there is no formal change management policy documented, or it is incomplete and lacks critical procedures."
- **Q1.2**: Does the policy clearly define the scope of changes?
    - **Positive**: "Yes, the policy clearly defines the scope of changes, covering software, hardware, network configurations, and user access controls."
    - **Negative**: "No, the policy does not clearly define the scope of changes, leading to inconsistencies in change management."
- **Q1.3**: Is a Change Advisory Board (CAB) established?
    - **Positive**: "Yes, a CAB is in place and responsible for reviewing and approving all changes."
    - **Negative**: "No, there is no CAB established, and changes are made without formal approval."
- **Q1.4**: Are all change requests documented and maintained for audit purposes?
    - **Positive**: "Yes, all change requests, approvals, and testing results are documented and archived for audits."
    - **Negative**: "No, documentation of change requests is inconsistent or missing, making audits difficult."
- **Q1.5**: Is the policy reviewed and updated periodically?
    - **Positive**: "Yes, the policy is reviewed and updated annually to align with regulatory and business requirements."
    - **Negative**: "No, the policy has not been reviewed or updated in the past two years."

2. Implement Role-Based Access Control (RBAC) for Change Management

- **Q2.1**: Is access to change management tools restricted based on roles and responsibilities?
    - **Positive**: "Yes, access to change management tools is restricted, and only authorized personnel have the necessary permissions."
    - **Negative**: "No, access is not adequately controlled, allowing unauthorized personnel to access and modify settings."
- **Q2.2**: Are RBAC policies implemented to ensure authorized personnel manage changes?
    - **Positive**: "Yes, RBAC policies are enforced to ensure only authorized personnel can initiate, review, or approve changes."
    - **Negative**: "No, RBAC policies are not in place, leading to potential unauthorized changes."
- **Q2.3**: Is there an up-to-date inventory of user roles and permissions?
    - **Positive**: "Yes, an inventory of user roles and permissions is maintained

and updated regularly."
    - **Negative**: "No, there is no current inventory of user roles, making it difficult to track permissions."
- **Q2.4**: Are periodic audits conducted to validate access permissions?
    - **Positive**: "Yes, periodic audits are conducted to review and validate access permissions, ensuring compliance with policies."
    - **Negative**: "No, access permissions are not audited, increasing the risk of unauthorized access."

3. Document and Track All Changes

- **Q3.1**: Is a ticketing system used to document and track all changes?
    - **Positive**: "Yes, a ticketing system (e.g., ServiceNow) is used to document and track all changes, including relevant details."
    - **Negative**: "No, there is no standardized system for tracking changes, leading to inconsistencies."
- **Q3.2**: Does the change documentation include necessary details like testing outcomes and rollback plans?
    - **Positive**: "Yes, all change requests include detailed information, including testing outcomes and rollback plans."
    - **Negative**: "No, change requests lack comprehensive details, affecting the ability to track and manage changes effectively."
- **Q3.3**: Are logs of approved and rejected changes maintained?
    - **Positive**: "Yes, logs of all approved and rejected changes are maintained and available for review."
    - **Negative**: "No, change logs are incomplete or not consistently maintained."
- **Q3.4**: Are rollback procedures documented in change requests?
    - **Positive**: "Yes, rollback procedures are documented as part of the change request process."
    - **Negative**: "No, rollback procedures are missing from change documentation."

4. Enforce Multi-Factor Authentication (MFA) for Externally Exposed Systems

- **Q4.1**: Is MFA implemented for all systems accessible externally?
    - **Positive**: "Yes, MFA is enforced for all externally accessible systems, including VPNs and cloud applications."
    - **Negative**: "No, MFA is not implemented for some or all externally accessible systems."
- **Q4.2**: Is MFA enforced consistently across all users?
    - **Positive**: "Yes, MFA is enforced consistently for all users, including privileged and administrative accounts."
    - **Negative**: "No, MFA enforcement is inconsistent, especially for privileged users."
- **Q4.3**: Are regular audits conducted to verify MFA implementation?
    - **Positive**: "Yes, regular audits are conducted to verify that MFA is properly configured and enforced."
    - **Negative**: "No, MFA implementation is not audited regularly, creating potential security gaps."

5. Conduct Regular Configuration Reviews

- **Q5.1**: Is there a process for reviewing system configurations regularly?
    - **Positive**: "Yes, system configurations are reviewed regularly as part of a structured process."
    - **Negative**: "No, system configurations are not reviewed regularly, increasing the risk of misconfigurations."
- **Q5.2**: Are baseline configurations maintained for all systems?
    - **Positive**: "Yes, baseline configurations are documented and maintained for all systems."
    - **Negative**: "No, baseline configurations are either not maintained or outdated."
- **Q5.3**: Are regular audits conducted for system configurations?
    - **Positive**: "Yes, regular audits of firewall rules, server settings, and access permissions are conducted."
    - **Negative**: "No, system configurations are not audited, which may lead to unmonitored deviations."
- **Q5.4**: Are automated tools used for configuration tracking?
    - **Positive**: "Yes, automated tools are deployed to track configuration changes and alert security teams of deviations."
    - **Negative**: "No, automated tools are not utilized, and configuration changes are tracked manually."

6. Develop and Maintain Configuration Management Procedures

- **Q6.1**: Are standard procedures for managing configurations documented?
    - **Positive**: "Yes, standard procedures for managing configurations are documented and regularly updated."
    - **Negative**: "No, there are no standardized procedures for configuration management."
- **Q6.2**: Are configurations validated before deployment?
    - **Positive**: "Yes, configurations are validated before deployment to ensure compliance with standards."
    - **Negative**: "No, configurations are not consistently validated before deployment."
- **Q6.3**: Are approved configurations documented?
    - **Positive**: "Yes, approved configurations are documented, and systems adhere to these standards."
    - **Negative**: "No, approved configurations are not properly documented."
- **Q6.4**: Is there a process for addressing misconfigurations?
    - **Positive**: "Yes, there is a process for promptly addressing and correcting misconfigurations."
    - **Negative**: "No, there is no process in place to address misconfigurations."

7. Perform Post-Implementation Reviews and Testing

- **Q7.1**: Are post-implementation reviews conducted to verify changes?
    - **Positive**: "Yes, post-implementation reviews are conducted for all changes to verify outcomes."
    - **Negative**: "No, changes are not consistently reviewed after implementation."
- **Q7.2**: Are system logs reviewed after changes?
    - **Positive**: "Yes, system logs are reviewed post-implementation to identify

issues."
    - **Negative**: "No, system logs are not reviewed after changes."

8. Enable Continuous Monitoring for Unauthorized Changes

- **Q8.1**: Are continuous monitoring tools deployed?
    - **Positive**: "Yes, continuous monitoring tools are deployed to detect unauthorized changes."
    - **Negative**: "No, continuous monitoring is not implemented."

9. Test Rollback and Contingency Plans

- **Q9.1**: Are rollback procedures established and tested?
    - **Positive**: "Yes, rollback procedures are documented and tested regularly."
    - **Negative**: "No, rollback procedures are not documented or tested."

10. Audit and Report Compliance with Change Management

- **Q10.1**: Are regular audits conducted?
    - **Positive**: "Yes, regular audits of the change management process are conducted."
    - **Negative**: "No, audits are not conducted regularly."
- **Q10.2**: Is a formal compliance report prepared?
    - **Positive**: "Yes, compliance reports are prepared and reviewed by the board."
    - **Negative**: "No, compliance reports are not prepared."

11. Implement Metrics for Monitoring Change Management Efficiency

- **Q11.1**: Are key metrics defined and monitored?
    - **Positive**: "Yes, key metrics are defined, monitored, and reported."
    - **Negative**: "No, metrics for monitoring change management are not defined."

Checklist

Thursday, October 10, 2024 3:59 PM

Checklist for Change Management Compliance Evaluation

1. Develop a Comprehensive Change Management Policy

- A formal, documented change management policy exists.
- The policy outlines procedures for requesting, reviewing, approving, and implementing changes.
- The policy clearly defines the scope of changes, including software, hardware, network configurations, and user access controls.
- A Change Advisory Board (CAB) is established and reviews all changes.
- Documentation of change requests, approvals, and testing results is maintained.
- The policy is reviewed and updated periodically (at least annually).

2. Implement Role-Based Access Control (RBAC) for Change Management

- Access to change management tools and configuration settings is restricted based on roles and responsibilities.
- An RBAC policy is implemented to ensure that only authorized personnel can manage changes.
- An up-to-date inventory of user roles, responsibilities, and permissions is maintained.
- Regular audits are conducted to review and validate access permissions.

3. Document and Track All Changes

- A ticketing system (e.g., ServiceNow, JIRA) is used to document and track all changes.
- Each change request includes details such as the requestor, affected systems, reason for change, and testing outcomes.
- Logs of all approved and rejected changes are maintained for audit purposes.
- Rollback procedures and contingency plans are included in change documentation.

4. Enforce Multi-Factor Authentication (MFA) for Externally Exposed Systems

- MFA is implemented for all systems that are accessible externally (VPNs, cloud apps, remote access points).
- MFA is enforced consistently across all users, including privileged accounts.
- Regular audits verify that MFA is properly configured and enforced.

5. Conduct Regular Configuration Reviews

- A regular review process for system configurations is in place.
- Baseline configurations for all systems are documented and maintained.
- Regular audits are conducted to review system configurations (e.g., firewall rules, server settings).
- Automated tools are deployed to track configuration changes and alert the security team of deviations.

6. Develop and Maintain Configuration Management Procedures

- Standard procedures for managing configurations are documented and maintained.
- Configurations are validated before deployment to ensure compliance with security standards.
- Approved configurations are documented, and systems adhere to these standards.

- A process is in place for promptly addressing and correcting misconfigurations.

7. Perform Post-Implementation Reviews and Testing

- Post-implementation reviews are conducted for all changes.
- Post-implementation testing is performed to verify the effectiveness of changes.
- System logs and performance metrics are reviewed after implementing changes.
- Results of post-implementation testing are documented and reported to the CAB.

8. Enable Continuous Monitoring for Unauthorized Changes

- Continuous monitoring tools (e.g., Splunk, SolarWinds) are deployed to detect unauthorized changes.
- Alerts are configured to notify the security team of unauthorized changes or access attempts.
- A regular log review process is in place to identify suspicious activities.
- All changes are logged and available for audit.

9. Test Rollback and Contingency Plans

- Rollback procedures are established for critical systems and changes.
- Tests are conducted regularly to verify rollback procedures' effectiveness.
- Rollback procedures are included in change documentation and reviewed for accuracy.
- Contingency plans are tested to verify their effectiveness in minimizing disruptions.

10. Audit and Report Compliance with Change Management

- Regular audits are scheduled to review the change management process for compliance with regulatory requirements.
- Internal or external auditors review the change management process.
- A formal report on change management compliance is prepared for the board and stakeholders.
- Audit findings are addressed through documented remediation plans.

11. Implement Metrics for Monitoring Change Management Efficiency

- Key metrics (e.g., number of approved/rejected changes, incidents from improper changes) are defined.
- Metrics such as time to approve changes or success rates are tracked.
- The results of these metrics are reported to the CAB and relevant stakeholders.
- Metrics are used to identify areas for improvement and optimize the change management process.

EF

Wednesday, December 4, 2024 9:16 AM

Finding: Unrestricted Code Execution and Lack of Preventative Controls
Regulatory Citation: 12 CFR Part 748, Appendix A, Section III – Safeguarding Member Information
Observation:
The credit union has not implemented sufficient controls to prevent unrestricted code execution within its information systems. This failure exposes the institution to significant risks, including the execution of malicious applications, unauthorized kernel-level operations, and exploitation of scripting environments.
Specifically:

1. System settings do not restrict the execution of applications downloaded from untrusted sources.
2. Application control tools (allowlisting) are not in place to limit program execution to authorized applications, nor do they validate key attributes such as digital signatures.
3. There is no evidence of controls to block the execution of known vulnerable drivers or a validation process for driver block rules in an audit environment prior to production deployment.
4. Scripting languages are unconstrained, and script logs are not being audited for potential malicious activities.
5. Containers used in the environment are not configured as read-only or minimal, increasing the risk of unauthorized command execution.
6. Protections, such as spam filtering and analysis of border and host-level security, have not been reviewed for effectiveness in blocking malware delivery.

Risk:
The lack of these controls compromises the credit union's ability to safeguard member information, as required under 12 CFR Part 748, Appendix A. This failure may allow adversaries to exploit system vulnerabilities, leading to unauthorized access, data breaches, and operational disruption.
Recommendations:
To address these gaps and comply with regulatory requirements, the credit union should:

1. **Enable Restrictive System Settings:** Configure system settings to block the execution of applications from untrusted sources.
2. **Implement Allowlisting:** Deploy application control tools that enforce allowlisting by default, ensuring only explicitly approved executable files can run. These tools should validate digital signatures and other key attributes.
3. **Enforce Driver Block Rules:** Develop and implement driver block rules to prevent execution of known vulnerable drivers and validate these rules in audit mode before production deployment.
4. **Constrain Scripting Languages:** Limit the use of scripting languages to essential business functions, audit script logs regularly, and restrict the execution of unnecessary scripting tools like PowerShell.
5. **Use Read-Only Containers:** Transition to using read-only and minimal containers to reduce the risk of unauthorized code execution.

6. **Analyze Protections:** Regularly assess spam filtering and host-level protections to ensure their continued effectiveness in blocking malware delivery. Reconfigure settings, such as remapping the default program for HTA files, where business requirements do not mandate their use.

Conclusion:

These measures are critical for reducing the risk of unauthorized code execution, safeguarding member information, and maintaining compliance with 12 CFR Part 748. Implementing these recommendations will strengthen the credit union’s information security posture and support its regulatory obligations.

PowerShell

Wednesday, January 22, 2025 9:48 AM

Enable PowerShell, Windows Remote Management, and WMI Auditing
Verify PowerShell v4.0 (at a minimum, preferably v5.1 or higher) is in use and that PowerShell logging is configured to support the collection of forensic and investigative artifacts. Lower versions of PowerShell should be uninstalled to prevent downgrade attack vectors.
Enhancing PowerShell, WinRM, and WMI logging and retention will require the following:

- Upgrade PowerShell to version 5.1 on all systems where it is installed
- Enable PowerShell Module Logging
- Enable PowerShell Script Block Logging
- Enable PowerShell Transcription
- Configure Maximum Log Size and log forwarding for related log files

Relevant log files include:

- Microsoft-Windows-PowerShell/Operational
- Microsoft-Windows-WinRM/Operational
- Microsoft-Windows-WMI-Activity/Operational

For Windows 7/8.1/2008/2012 systems, upgrading PowerShell to version PowerShell 5.1 (recommended) requires:

- .NET 4.5.2+
- Windows Management Framework (WMF) 5.1

Details on upgrade paths can be found here: https://docs.microsoft.com/en-us/powershell/scripting/windows-powershell/wmf/setup/install-configure

To enable PowerShell Module Logging

Open Group Policy and navigate to:

```
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell
    > Turn on Module Logging
        > Enabled
```

Figure 5: Group Policy path for PowerShell Module Logging

In the options pane, click the button to show `Module Name`

1. In the `Module Names` window, enter "*" to record all modules
2. Click `OK` in the `Module Names` Window
3. Click `OK` in the `Module Logging` Window

To enable PowerShell Script Block Logging

1. Open Group Policy and navigate to:

```
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell
    > Turn on PowerShell Script Block Logging
        > Enabled
```

Figure 6: Group Policy path for PowerShell Script Block Logging

To enable PowerShell Transcription

1. Open Group Policy and navigate to:

```
Computer Configuration > Policies > Administrative Templates > Windows Components >
```

```
Windows PowerShell
    > Turn on PowerShell Transcription
        > Enabled
```

Figure 7: Group Policy path for PowerShell Transcription

1. Check the Include invocation headers box
2. Optionally, set a centralized transcript output directory

To disable PowerShell 2.0 on Windows 8.1 (and above) and Windows Server 2012 (and above)

From an elevated command prompt (or within a script), run the command noted in Figure 8

```
DISM /online /disable-feature /featurename: Disable-WindowsOptionalFeature -Online -
FeatureName MicrosoftWindowsPowerShellV2Root
```

Figure 8: Command to disable PowerShell 2.0

From an elevated PowerShell session (or within a PowerShell script), run the command noted in Figure 9.

```
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root
```

Figure 9: Optional command to disable PowerShell 2.0

Enhancing visibility for PowerShell activity provides improved detection and correlation for events that may be malicious or suspicious. Many attackers now utilize PowerShell to invoke malicious activity, laterally move, and configure persistent mechanisms for leveraging access within an enterprise environment.

Even if verbose PowerShell logs are not forwarded to a SIEM for non-critical systems (e.g., end-user workstations, laptops, non-critical servers), the ability to capture this level of information locally on the endpoint would ensure that detailed logging is available in the event of an investigation.

Ensure Logging of Command Line Process Creation Events

Ensure that process tracking is enabled in the security event logs (Event ID 4688) for all endpoints, and that the command line history is being recorded for these events on each endpoint.

This feature can be enabled by installing KB3004375 and configuring the Group Policy setting noted below:

1. `Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation > Include command line in process creation events`

   KB3004375: https://www.microsoft.com/en-us/download/details.aspx?id=45627

   For additional information, reference:

2. https://support.microsoft.com/en-us/kb/3004375
3. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

Capturing process creation events improves the likelihood of determining what an attacker accomplished on an endpoint. Enhancing visibility for command line arguments that are utilized to initiate processes provides improved detection and correlation for condition that may be malicious or suspicious. This level of visibility also enhances detection of suspicious events by generating alerts based upon pre-defined patterns of common attacker activity.

Notes

Tuesday, August 13, 2024 3:33 PM

The review of the change and configuration management processes confirmed compliance with **12 CFR 748.0**and **Appendix A to Part 748**by establishing a comprehensive change management policy, implementing role-based access control (RBAC), and enforcing multi-factor authentication (MFA) for externally accessible systems. All changes were documented and tracked using a ticketing system, including details on requestors, affected systems, testing outcomes, and rollback procedures, with logs maintained for audit purposes. Baseline configurations were developed and regularly reviewed using automated tools to track deviations, and misconfigurations were addressed promptly. Post-implementation reviews and testing verified that changes achieved desired outcomes without introducing vulnerabilities, while continuous monitoring tools detected unauthorized changes. Rollback and contingency plans were tested to mitigate unintended effects, and regular audits ensured compliance with regulatory requirements, with findings reported to the board of directors. Metrics were tracked to assess the efficiency and effectiveness of the change management process, supporting continuous improvement and safeguarding sensitive member information.