cenareo

Cyber Security - Vulnerability Management

This policy outlines the formal procedures for vulnerability & patch management within Cenareo.

It ensures timely identification, prioritization, and deployment of security patches for all applications and systems processing data.

This policy is subject to periodic review and updates to reflect changes in technology, industry best practices, and regulatory requirements.

Responsibilities

- **Information Security Team**: Responsible for managing the vulnerability scanner, risk assessment process, reporting, and overall program effectiveness.
- **IT Operations Team**: Responsible for deployment of patches according to the established schedule, testing of critical and high-severity patches (if required), and communication with system owners.
- **System Owners**: Responsible for ensuring timely application of patches to their respective systems and collaborating with the IT Operations team during emergency patch deployments.

Vulnerability Management

Vulnerability Scanning

We conduct regular vulnerability scans of our information systems processing customer data, both internally and externally. This includes a combination of automated vulnerability scanning tools and manual penetration testing.

Frequency

- **Network Level Vulnerability Scans**: We perform network vulnerability scans at least quarterly, with additional scans conducted if critical vulnerabilities are identified or significant changes are made to the network infrastructure.
- **OS Level Vulnerability Scans**: Operating system vulnerability scans are conducted at least monthly.
- **Application Level Vulnerability Scans**: Application vulnerability scans are performed regularly, with the frequency depending on the criticality of the application and the frequency of updates or changes. High-risk applications may be scanned weekly or even more frequently.

cenareo

Penetration Testing

We conduct both internal and external penetration tests of our service infrastructure servicing customer data.

Internal Penetration Testing

Red team exercises are simulated attacks conducted by a dedicated security team to identify vulnerabilities within our systems and processes. These exercises are performed at least annually.

External Network Penetration Testing

We engage independent security firms to conduct external penetration tests of our service infrastructure at least annually.

Additional Information

The specific frequency of vulnerability scans and penetration testing may be adjusted based on risk assessments and industry best practices. We prioritize the remediation of vulnerabilities based on severity, exploitability, and potential impact on our systems and data. We maintain a vulnerability management program to track identified vulnerabilities, their remediation status, and retesting efforts.

Patch Management

Patch Management Procedures

Inventory and Classification

We maintain a comprehensive inventory of all software applications and operating systems used within the company. Each application and system will be classified based on its criticality and the type of data it processes.

Vulnerability Management

We utilize a vulnerability scanning tool to identify known security vulnerabilities in our software and systems. We will regularly update the vulnerability scanner with the latest vulnerability information.

Risk Rating Process

Identified vulnerabilities will be assessed for risk based on severity (critical, high, medium, low), exploitability, and the potential impact on our systems and data.

Patch Deployment Schedule

- **Critical Vulnerabilities**: Patches for critical vulnerabilities will be deployed within 24 hours of confirmation.
- **High Severity Vulnerabilities**: Patches for high-severity vulnerabilities will be deployed within 72 hours of confirmation.
- **Medium and Low Severity Vulnerabilities**: Patches for medium and low severity vulnerabilities will be addressed according to a risk-based schedule, with priority given to vulnerabilities affecting critical systems or those with a high exploitability rating.

Testing and Approval

Before deployment on production systems, critical and high-severity patches may undergo limited internal testing to ensure minimal disruption to operations.

Deployment and Verification

Patches will be deployed to all affected systems following the established schedule.
Successful deployment and patch application will be verified.

Emergency Patch Implementation Process

In the event of a zero-day attack or a critical vulnerability with a high exploitability rating, an emergency patch deployment process will be initiated.

This process will involve:

- **Rapid Risk Assessment**: The Information Security team will conduct a rapid risk assessment of the vulnerability.
- **Emergency Patch Acquisition and Testing**: IT Operations will prioritize obtaining and, if necessary, conducting limited testing of the emergency patch.
- **Deployment Authorization**: The Information Security team, in consultation with relevant stakeholders, will authorize the deployment of the emergency patch.
- **Deployment and Communication**: The IT Operations team will deploy the emergency patch to affected systems. All relevant personnel will be notified of the emergency patch deployment and any potential impacts.

Reporting and Monitoring

The Information Security team maintains records of all identified vulnerabilities, risk assessments, patch deployments, and emergency response procedures.

Regular reports will be generated to monitor the effectiveness of the patch management program and identify areas for improvement.

Server Security Standard

This section outlines server security hardening standards for all servers within Cenareo organization.

These standards are designed to minimize the attack surface and reduce the risk of unauthorized access, data breaches, and system disruptions.

This standard specifically emphasizes the importance of patch management as a critical aspect of server security.

Server Hardening Principles

Minimize Installed Software

Only install software applications and services that are necessary for server functionality. Remove any unused or unnecessary software components to reduce the potential attack surface.

Keep Software Up-to-Date

Apply security patches promptly upon release from the vendor. Prioritize patching critical vulnerabilities first. Utilize a centralized patch management solution to automate and streamline the patching process whenever possible.

Secure Default Accounts

Disable unused default accounts provided by the operating system or software applications. Rename or disable administrator accounts with generic names like "admin" or "root".

Enforce Strong Passwords

Implement strong password policies that require complex passwords with a minimum length and enforce regular password changes. Consider multi-factor authentication (MFA) for additional security.

Restrict Administrative Access

Limit administrative access to servers using the principle of least privilege. Grant users only the minimum permissions required to perform their assigned tasks.

Configure Firewalls

Configure firewalls to restrict inbound and outbound traffic to only authorized ports and protocols.

Disable Unnecessary Services

Disable any services that are not essential for server operation. This reduces the attack surface and potential vulnerabilities.

Audit and Log Activity

Enable system logging and regularly review logs for suspicious activity.

Regular Security Assessments

Conduct periodic security assessments of servers to identify and address any security weaknesses.

Patch Management Procedures

Centralized Patch Management

Whenever possible, utilize a centralized patch management solution to automate patch deployment across all servers. This ensures efficient and consistent patching across the environment.

Vulnerability Assessment and Prioritization

Regularly scan servers for vulnerabilities using vulnerability scanning tools. Prioritize patching critical vulnerabilities based on severity and potential risk.

Testing

Before deploying patches to production servers, conduct thorough testing in a staging environment to minimize the risk of introducing compatibility issues or system disruptions.

Patch Deployment Schedule

Establish a regular patch deployment schedule. Consider deploying critical security patches immediately, while balancing with planned maintenance windows for less critical updates.

Post-Patching Verification

Verify the successful deployment and functionality of patches after installation. Monitor systems for any unexpected behavior or issues.

Documentation

Maintain detailed documentation of all installed software, patch versions, and deployment dates for each server.

Additional Considerations

- **Third-Party Applications:** Third-party applications installed on servers are kept up-to-date with security patches from their respective vendors.
- **End-of-Life (EOL) Software:** No outdated software that no longer receives security updates from the vendor with anticipated plans to migrate away from EOL software to supported versions or alternative solutions.
- **Physical Security:** access control server hardware and unauthorized access prevention.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650