elevaite365

TECH THAT MATTERS

Elevaite365

IT Hardening Guidelines

Version 1.0

PURPOSE

The IT Hardening Guidelines aim to establish standardized procedures and best practices for securing the organization's IT systems and infrastructure. This policy aims to reduce vulnerabilities, protect against unauthorized access, and ensure information assets' integrity, confidentiality, and availability by implementing robust security measures.

SCOPE

This policy applies to all IT systems, servers, networks, applications, and devices owned, operated, or managed by Elevaite365 (hereby as organization). It encompasses hardware, software, firmware, and all related components within the organization's IT infrastructure. Additionally, it applies to all employees, contractors, consultants, and third-party partners who interact with these systems.

DEFINITIONS

1. IT Hardening: Securing IT systems by reducing their surface vulnerability through configuration and removing unnecessary services, applications, and features.
2. Vulnerability: A system's weakness that threats can exploit to gain unauthorized access or cause harm.
3. Patch Management: Managing updates for software applications and technologies to fix vulnerabilities.
4. Baseline Configuration: A set of specifications for a system that serves as a basis for its secure configuration.
5. Access Control: Mechanisms that restrict access to information systems and resources to authorized users only.
6. Firewall: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
7. Antivirus Software: Programs designed to detect, prevent, and remove malware from IT systems.
8. Encryption is converting information or data into a code to prevent unauthorized access.
9. Multi-Factor Authentication (MFA): A security system requiring multiple authentication methods to verify a user's identity.
10. Zero-Day Vulnerability: A security flaw unknown to the party responsible for patching or otherwise fixing the flaw.

POLICY

General Hardening Practices

1. **Baseline Configuration:**
   a. Establish and maintain baseline configurations for all IT systems, including servers, workstations, and network devices.
   b. Ensure that configurations comply with industry best practices and organizational security standards.
2. **Minimize Installed Services and Applications:**
   a. Remove or turn off unnecessary services, applications, and features to reduce potential attack vectors.
   b. Regularly review installed software and services to ensure only essential components are active.
3. **Patch Management:**
   a. Implement a robust patch management process to ensure timely updates and patches for all software and firmware.
   b. Prioritize patch deployment based on the severity of vulnerabilities and potential impact on the organization.
4. **Access Control:**
   a. Enforce the principle of least privilege, ensuring users have only the access necessary to perform their job functions.
   b. Implement role-based access controls (RBAC) to manage permissions systematically.
5. **Firewall Configuration:**
   a. Configure firewalls to restrict unauthorized access to and from the network.
   b. Regularly review and update firewall rules to adapt to changing security requirements.
6. **Antivirus and Anti-Malware Protection:**
   a. Deploy reputable antivirus and anti-malware solutions on all endpoints.
   b. Ensure that these solutions are regularly updated and configured to perform automatic scans.
7. **Encryption:**
   a. Utilize encryption for sensitive data both at rest and in transit.
   b. Ensure encryption keys are managed securely and rotated regularly.
8. **Logging and Monitoring:**
   a. Enable detailed logging on all critical systems and network devices.
   b. Implement continuous monitoring to detect and respond to suspicious activities promptly.

9. **Multi-Factor Authentication (MFA):**
   a. Require MFA for accessing critical systems and applications, especially for remote access and administrative accounts.
   b. Ensure that MFA mechanisms are robust and regularly evaluated for effectiveness.
10. **Secure Configuration Management:**
   a. Document all configurations and changes to IT systems.
   b. Use configuration management tools to enforce and maintain secure settings across the IT infrastructure.

Server Hardening

1. **Operating System Hardening:**
   a. Disable or remove unnecessary services and ports.
   b. Apply the latest security patches and updates.
   c. Configure strong password policies and account lockout mechanisms.
2. **Application Hardening:**
   a. Remove or turn off unused features and components in applications.
   b. Implement application-level firewalls and security controls.
3. **User Account Management:**
   a. Ensure that all user accounts are unique and properly managed.
   b. Regularly review and audit user accounts and permissions.

Network Hardening

1. **Segmentation:**
   a. Segment the network to isolate critical systems and data from less secure areas.
   b. Use VLANs and subnetting to enforce network segmentation effectively.
2. **Intrusion Detection and Prevention Systems (IDPS):**
   a. Deploy IDPS to monitor network traffic for malicious activities.
   b. Configure IDPS to respond automatically to detected threats when appropriate.
3. **Secure Wireless Configurations:**
   a. Implement strong encryption protocols (e.g., WPA3) for all wireless networks.
   b. Disable broadcasting of network SSIDs and implement MAC address filtering where feasible.

Endpoint Hardening

1. **Workstation Security:**
   a. Enforce secure boot processes and BIOS/UEFI configurations.
   b. Implement full disk encryption on all endpoints.
2. **Mobile Device Management (MDM):**
   a. Deploy MDM solutions to manage and secure mobile devices.
   b. Enforce policies for device encryption, remote wipe, and secure access.

Application Hardening

1. **Secure Development Practices:**
   a. Integrate security into the software development lifecycle (SDLC).
   b. Conduct regular code reviews and security testing (e.g., static and dynamic analysis).
2. **Web Application Security:**
   a. Implement Web Application Firewalls (WAF) to protect against common web threats.
   b. Enforce secure coding standards to mitigate vulnerabilities like SQL injection and cross-site scripting (XSS).

USER PASSWORD COMPLEXITY

Cloud Infrastructure

1. Passwords must contain at least 10 Characters , including at least one uppercase letter, one lowercase letter, one number, and one unique character.
2. Multi-factor authentication must be enabled for all Personnel accessing the production environment in the cloud.
3. Password and user IDs must not be identical.
4. Passwords must not contain personal information, such as birthdays, names, addresses, or phone numbers.

5. Passwords must not be easily guessable by third parties or automated software. Any new password must differ from the previous three (3) passwords.
6. All passwords will expire after 180 Days .

Passwords for Email, End-Points, and Web Applications

1. Passwords must contain at least 10 Characters, including at least one uppercase letter, one lowercase letter, 1 number, and one unique character.

2. Password and user IDs must not be identical.

3. Passwords must not contain personal information, such as birthdays, names, addresses, or phone numbers.

4. Passwords must not be easily guessable by third parties or automated software. Any new password must differ from the previous three (3) passwords.

5. All passwords will expire after 180 Days .

PERFORM VULNERABILITY SCAN

1. The system will be scanned with a vulnerability scanner. Any vulnerabilities discovered will be resolved.
2. If no significant vulnerabilities exist, the system can be prepared for live use.
3. Any new service, server, device, or application will undergo a vulnerability assessment scan, and any discovered vulnerabilities will be resolved before such service, server, device, or application goes live.

AWS/Azure/GCP HARDENING GUIDELINES

AWS Hardening will follow the CIS Amazon Web Services Foundations Benchmark V1.4.0. https://docs.aws.amazon.com/securityhub/latest/userguide/cis-aws-foundations- benchmark.html#cis1v4-standard

Azure Hardening checklist: https://learn.microsoft.com/en- us/azure/security/fundamentals/operational-checklist

GCP: https://cloud.google.com/security/best-practices

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan,Linh	Linh	Borhan