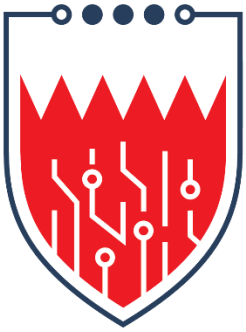

المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

Protect Your Organization

Table of Contents

Recommendations

Recommendations

Critical

- Ensure MFA and strong passwords are enforced.
- Ensure regular backup of important data.
- Ensure patching is automated and all systems and server components are updated.

Important

- Ensure network segmentation is implemented.
- Ensure IDS/IPS and WAF are deployed and configured.
- Ensure unused ports and services are disabled.
- Ensure logging and monitoring are enabled.
- Ensure RDP/SSH access is restricted.
- Ensure Principle of Least Privilege is applied.
- Ensure inactive and default accounts are removed.
- Ensure EDR/XDR and endpoint protection deployed and up to date.
- Ensure USB, macros, and scripting tools are restricted.
- Ensure vulnerability assessments are regularly conducted, especially on internet-facing systems.
- Ensure OWASP's Top 10 is followed for web application security.
- Ensure directory traversal is restricted on websites.
- Ensure services run under service accounts, not administrator accounts.
- Ensure user's permissions are periodically reviewed.
- Ensure brute force attack protection is in place by limiting login attempts.
- Ensure DNS filtering is configured.
- Ensure employees are educated on cybersecurity threats and best practices.

Protecting Against DDoS

Protecting Against DDoS

General Recommendations

- Implementing robust security measures to identify and block malicious traffic before it reaches the network.
- Regular security audits are important to identify vulnerabilities in the environment and to ensure that security measures are up to date.
- Monitoring network traffic can help to identify patterns that may indicate a DDoS attack.
- Load balancing is an effective way to prevent DDoS attacks by distributing traffic across multiple servers.
- Employee education is an important part of protecting the environment from DDoS attacks. Employees should be trained on how to recognize and report suspicious activity.
- Collaboration with other organizations can help to share knowledge and resources to prevent DDoS attacks.
- Keeping software up to date is important to prevent vulnerabilities that can be exploited by attackers.
- Implement real-time traffic analysis and filtering to identify and block malicious requests.
- Integrate with Web Application Firewalls (WAFs) to protect against application layer attacks.
- Regularly monitor and analyze DDoS attack data to refine security strategies and improve defenses.

Cloud Recommendations

- Enable auto-scaling for the nodes to seamlessly manage both scale-up and scale-down operations.
- Leverage cloud-based DDoS protection services that offer scalable and resilient defense against attacks.
- Utilize a global Anycast network to distribute and filter incoming traffic.
- Employ automated mitigation techniques, such as rate limiting and traffic redirection, to counter DDoS attacks.

Protecting Against Ransomware

Protecting Against Ransomware

Quick Wins

- Avoid using similar syntax/pattern in passwords on service/administrator accounts. Obtaining one password by the threat actor will make the process of cracking the rest easy using dictionary attacks.
- Regularly change all passwords, including passwords to service accounts, while ensuring compliance to strong and complex password policy.
- Disable Microsoft Office macro scripts, as these macros can be used to deliver ransomware.
- Restrict the use of PowerShell to specific users. Use Group Policy to specify usage for each user.
- Improve the user's awareness of phishing emails and other suspicious activities.
- patch and update operating systems and software to the latest available versions regularly.
- Restrict the use of USB drives or other removable devices.

Intermediate Guidelines

Data protection

- Use offline encrypted backups, especially for critical and sensitive data. Regularly test and maintain backups.

Human resources

- Have a dedicated security officer or team that is responsible of governance, risk and compliance (GRC).
- Have adequate resources to manage and operate the implemented systems and security controls.

Endpoint protection

- Perform regular vulnerability assessments on all systems, especially those on internet-facing systems. Security vulnerabilities, including weak passwords and misconfigurations, can help threat actors bypass security.
- Implement the principle of least privilege where users and system services are given privileges needed to complete their tasks. Separate accounts should be used for tasks requiring higher privilege. It is recommended to use Privileged Access Manager and

Endpoint Privilege Manager or similar solutions. These limit and control such privileged access across systems and endpoints.

- Implement Privileged Access Workstations (PAWs), which are dedicated workstations for IT administrators that are used for tasks that require using highly privileged accounts so that other tasks, such as using email or web browsing, are done on other workstations.
- Enable multi-factor authentication (MFA) for all accounts, especially high privileged accounts.
- Implement a strict web browsing policy that prevents access to malicious websites.
- Disable or block inbound and outbound Server Message Block (SMB) protocol, as well as remove or disable outdated versions of SMB.
- Adversaries often target Domain Controllers (DCs) to spread ransomware network-wide. Therefore, securing domain controllers by restricting access to them is important.

Network protection

- Monitor network traffic for anomalies or suspicious activities.
- Implement network segmentation to separate various business units or IT resources within the organization and maintain separation between IT and operational technology. Network segmentation minimizes the impact of network intrusion and ransomware infections.
- RDP traffic should be monitored and restricted. Some RDP uses that should be blocked include RDP between servers, RDP from non-admin computers, and RDP directly from the internet. Threat actors often gain access to a network through exposed and poorly secured remote services, which results in a ransomware attack.
- Control traffic flow between an organization's network and backup/DR environments. In most cases, the traffic would be only in one direction and during specific times for backup purposes.

Monitoring Requirement

- Regularly review server logs for suspicious behavior and configure the servers to forward logs to a different server using log event management system. These logs should be monitored and correlated around the clock to address any suspicious events and to have records in case of any incident.

Technology Guidelines

- Implement an endpoint protection solution, such as an Endpoint Detection and Response (EDR) solution, to prevent infections or detect them early.
- Implement an email security solution that can detect and block malicious emails and attachments.
- Implement a Network Access Control (NAC) solution so that devices connected to the network are isolated if they are not compliant to the organization's security policy. This can reduce the risk of having cyber threats or infections from unauthorized devices connected to the network.

Protecting Against Web Defacement

Protecting Against Web Defacement

Web Application & Server Security

- Regularly update and patch CMS platforms, plugins, and web servers to fix known vulnerabilities.
- Disable or remove unused CMS features, themes, and plugins to minimize attack surfaces.
- Deploy a Web Application Firewall (WAF) to block malicious traffic and common web attacks.
- Enforce a Content Security Policy (CSP) to prevent unauthorized script execution.

Access Control & Authentication

- Implement Multi-Factor Authentication (MFA) for all administrative and privileged accounts.
- Restrict access to website administration panels using IP allowlisting or VPN-based access.
- Enforce strong, unique passwords and prevent password reuse across different services.

Secure Web Development Practices

- Apply input validation and sanitization to prevent SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- Follow the Principle of Least Privilege (PoLP) for database and website user accounts.
- Restrict file uploads to trusted formats and scan them for malware before processing.

Network & Server Hardening

- Configure intrusion detection and prevention systems (IDS/IPS) to monitor and block suspicious activity.
- Set correct file and directory permissions to prevent unauthorized modifications.
- Disable directory listing to prevent attackers from discovering sensitive files.

Backup & Recovery

- Maintain regular backups of website files and databases, stored securely and offline.
- Automate backup integrity testing to ensure quick restoration.

Monitoring & Detection

- Deploy File Integrity Monitoring (FIM) to detect unauthorized modifications.
- Implement real-time website monitoring to detect and alert on unexpected changes.
- Utilize CDNs with DDoS protection to mitigate attacks that may lead to defacement.