WEBROOT® PARTNER TRAINING

INTERNAL SECURITY BEST PRACTICES

NETWORK SECURITY CHECKLIST

Use this resource to evaluate, document, and reflect on the status of your network security. Contrast your findings with Webroot's recommended preventative measures in the Internal Security Best Practices content. What are your gaps? How might you solve for them?

GENERAL MEASURES

Multi-Vector Endpoint Security Solution

Use a proven, reputable endpoint security solution that offers realtime endpoint monitoring, and a thorough multi-vector protection approach.

3-2-1 Backup and Recovery Strategy

Keep at least **three** copies of your data, on at least **two** different storage types, with at least **one** copy of the data offsite.

Inventory and Patch Management Strategy

Develop a comprehensive list of all equipment and software in use by IT and end users, keep software updated, and address outdated hardware which may not be able to be updated with security patches.

Conduct Security Auditing

Leverage globally-accepted security standards and/or reputable software management solutions to ensure user permissions are correct, security software is installed and functioning correctly on endpoints, and that remote access is properly regulated for your network. Consider hiring a penetration tester to evaluate your vulnerable attack vectors.

Educate Yourself and Your Users

Engage yourself and end users with security awareness training and threat susceptibility testing (like phishing simulation). Educate yourself on latest threat trends, vulnerabilities, and exploits through software security events and industry professionals on social media.

SPECIFIC MEASURES

Disable Script File Executions

When possible, disable script file executions on user endpoints as they represent a massive network attack vector.

- **Disable WSF, WSH, HTA, VBS, and JS Files** via GPO, Webroot Management Console, or manually.
- **Disable Microsoft Office Macros** via GPO or manually.
- **Prevent users from running PowerShell** via GPO.

Restrict Remote Desktop Access

Consider restricting RDP access to a whitelisted IP or IP range, or preventing access altogether for some users. Enforce strong password and username requirements. Leverage two-factor authentication (like Smart Cards). Defend against brute force attacks with account lockout settings.

Management Console Best Practices

There are a variety of best practices to familiarize yourself with, but Overrides and Policies in particular need to be mentioned:

- Review whitelists in Overrides. Consider contacting Support for single MD5s - they can change rapidly.
- Ensure endpoints are not being managed in "Silent Audit" or "Unmanaged" policy states unneccesarily.

LEARN MORE

Use these resources to learn about processes and opportunities that can help with implementing preventative security meaures in your network.

- Malware Prevention Guide
- ISO/IEC 27001 Certification
- Webroot Business User Guides
- Webroot 2019 Threat Report
- CISSP Certification
- OWASP Foundation Homepage
- Webroot Industry Intel Blog
- Webroot Partner Certification
- Asset Management Solutions