LOCKDOWN LESSONS

WEBROOT Smarter Cybersecurity®

Closing Security Gaps

We can all agree: it's the nature of technology to advance. Cybercrime is no exception to this rule, and neither are the tools we use to stop attacks. But you'd be surprised how much a business can accomplish in terms of their own security simply by keeping existing systems up to date and using technology to their best advantage. For instance, just staying on top of patches and disabling unnecessary services that may be on by default can go a long way toward closing security gaps.

In this guide, we'll go over some basic ways that can help small and medium-sized businesses and managed service providers (MSPs) future-proof their IT environments against sophisticated, modern malware.

Patch and Keep Systems Up to Date

Unpatched software, operating systems, and firmware are a common vulnerability. For example, you only have to look at some of the major ransomware attacks that have made headlines. By exploiting security gaps in older operating systems, like when the WannaCry ransomware attack took advantage of the EternalBlue exploit in 2017, ransomware can spread like wildfire.

> **Malware can easily be distributed via exploit kits, which target the software vulnerabilities of older Windows® operating systems, Adobe® Flash Player, Oracle® Java, Microsoft® Internet Explorer, Microsoft® Silverlight, and other vulnerable applications.**

If this happens, an exploit kit landing page can execute arbitrary code and initiate a silent drive-by download. It is critical for system administrators to keep this type of software up to date as most infections dropped by exploit kits are zero-day threats, meaning they are never-before-seen unique samples that make it very hard for antivirus solutions to identify and block them before they can execute.

Restrict Remote Desktop Protocol Access

Cybercriminals are constantly on the lookout for systems with commonly used remote desktop protocol (RDP) ports. They then attack them using brute-force tactics, hoping to break through weak usernames and passwords and access systems.

> **Once criminals gain access, they can disable protection, deploy ransomware, create fraudulent user accounts, and much more.**

The following steps can help you secure RDP and prevent this type of attack:

- Restrict RDP to a whitelisted IP or IP range
- Require two-factor authentication, such as smart cards
- Use protection software to prevent RDP brute-force attacks
- Change the default RDP port from 3389 to another unused port
- Block RDP entirely (port 3389) via firewall
- Create a GPO to enforce strong password requirements
- Monitor possible intrusions using the Windows® Event Viewer (filter event logs by Event ID 4625, "an account failed to log on")

BECAUSE MANY MALWARE VARIANTS CAN BE DELIVERED THROUGH EMAIL ATTACHMENTS, TYPICALLY A ZIP ARCHIVE THAT CONTAINS A SCRIPT, YOU CAN HELP PREVENT ATTACKS SIMPLY BY DISABLING SCRIPTS, INCLUDING WSF, VBS, WSH, HTA, VBS AND JS FILES.

Block Known Malware Extensions and Disable Scripts and Macros

One of the simpler ways to use your own operating system to help prevent malware is to block certain file extensions that ransomware and other types of malware are known to use. You can run the file server resource manager (FSRM) to help classify files and block known malicious extensions.

Below are two methods you can use to block scripts.

- **Redirect script file extensions via GPO**
  This method lets you set the default program to open scripts. We recommend you redirect the following file types: .hta, .jse, .js, .vbs, .vbe, .wsf, .wsh, and .ps1.
- **Disable Microsoft® Windows® Script Host (WSH)**
  The wscript host is a Windows application that interprets and executes .vbs, .vbe, .js, .jse, .wsf and other types of script files. Depending on your IT needs, you may choose to disable it entirely.

As a further security measure, we recommend you consider disabling macros. While Microsoft® Office macros may have legitimate uses in your specific environment, they are typically not necessary; and can present a significant security risk, since some ransomware types use macros in documents as a method to deliver malicious payloads.

Invest in Intelligent Technology

If you've been paying attention to cybersecurity in the last few years, you know that artificial intelligence (AI) and machine learning (ML) aren't just buzz words, they're highly necessary for stopping zero-day threats. While these technologies may not fall into the category of using what you already have at hand, as the previous tips did, they do go a long way toward future-proofing your protection strategy.

> **With AI and machine learning, you can stop threats faster and with fewer false positives, and also improve productivity and business efficiency.**

By implementing intelligent security that uses AI and ML-powered detection, you can actually stop threats proactively through advanced behavioral analysis and contextual data. You can shorten the time it takes to detect and remediate threats, and, thereby, reduce the cost and impact associated with an attack. Finally, you can effectively augment your workforce by using these technologies to automate basic tasks, so employees are free to focus on other revenue-generating activities.

To see the next-gen, predictive Webroot approach to automated endpoint threat detection and response, DNS-layer security, and security awareness training, visit www.webroot.com.

To see how Carbonite backup and disaster recovery can help you gain peace of mind with complete protection from data loss, visit www.carbonite.com.