BARKLY BEST PRACTICES

2018 Cybersecurity Checklist

Is Your Company Protected from the Latest Attack Techniques?

Preventing Initial Compromise

The best defense against cyber attacks is to prevent attackers from gaining initial access to a machine in the first place.

VULNERABLE SOFTWARE

☐ **Patch What You Can**

When vulnerabilities are disclosed, it's only a matter of time before attackers begin exploiting them. Having a system in place to assess, test, and roll out patches is a vital first defense against attacks.

☐ **Isolate What You Can't**

Patching is vital, but not easy. Isolate systems you can't patch quickly by restricting network access.

EXPOSED PORTS & SERVICES

☐ **Secure Remote Desktop (RDP)**

Open ports with RDP exposed to the Internet are beacons for attackers. Restrict access to RDP listening ports by placing them behind a firewall and using a RDP Gateway. Enabling network-level authentication and changing the default listening port (TCP 3389) is also recommended.

☐ **Secure Server Message Block (SMB)**

Disable SMBv1 and use firewalls to restrict SMB network activity. WannaCry and other attacks leveraging the EternalBlue exploit have shown just how vulnerable organizations become when exposing SMB.

EMAIL

☐ **Block Common Malicious File Attachments**

In addition to the obvious (.EXE, .BAT), consider blocking script files (.JS, .VBS, etc.), archive files (.ZIP, .SFX, .7z), and even Office files (.DOC, .DOCX, etc.) and PDFs.

☐ **Conduct User Awareness Training**

Many attacks still initially require users clicking something they shouldn't. Training and inform your end-users about attacks that rely on deception and social engineering.

BROWSERS

☐ **Utilize Ad-Blockers**

Even legitimate websites can serve as infection points thanks to malvertising.

MICROSOFT OFFICE

☐ **Enforce Stricter Macro Controls**

Block macros in Office files downloaded from the Internet. Macros are abused to download malware and launch malicious scripts.

☐ **Disable "Update Automatic Links At Open" in Microsoft Word**

This will prevent abuse of the DDE feature (now disabled by default) and similar threats.

☐ **Disable OLE Packages**

Considering the long history of attackers abusing Microsoft's object linking and embedding (OLE) feature, it's best disabled when possible.

ALL OF THE ABOVE

☐ **Use Barkly's Endpoint Protection Platform**

Barkly prevents more attacks from successfully launching from any of these vectors. Learn more at barkly.com.

2018 Cybersecurity Checklist

Mitigating Post-Exploitation Techniques

Once attackers have access to a machine, they can evade detection by using fileless techniques and legitimate system administration tools to do their dirty work.

WHEN POWERSHELL ISN'T NECESSARY

- ☐ **Disable It**
  PowerShell is a powerful scripting framework that can provide attackers with a wide variety of dangerous functionality.

WHEN POWERSHELL IS NECESSARY

- ☐ **Update to Latest Version of PowerShell**
  It provides additional logging and updates to security features that can otherwise be bypassed on older versions (specifically version 2).
- ☐ **Block Unsigned PowerShell Scripts**
  While attackers can bypass this and other execution policy, attempts to do so can make attacks more visible.
- ☐ **Consider Using PowerShell Constrained Language Mode**
  It limits PowerShell to basic functionality, which will make many fileless attack techniques unusable.
- ☐ **Enable and Monitor Extended PowerShell Logging**
  Just be prepared for this to generate a lot of events. Tools like PowerShell Method Auditor can help process them.

SECURE & UTILIZE WINDOWS MANAGEMENT INSTRUMENTATION (WMI)

- ☐ **Create Defensive Permanent WMI Event Subscriptions**
  Its wide range of powerful admin capabilities make WMI a popular target of abuse, but they also make it a great tool for logging and responding to malicious activity. See examples here and here.
- ☐ **If There's No Need for Remote WMI**
  Consider setting up a fixed port for WMI and blocking it.

APPLY APPLICATION CONTROLS

- ☐ **Limit the Execution of Executables, DLLs, and Scripts with AppLocker**
  How restrictive you can be with whitelisting will depend on your organization's needs.
- ☐ **Take Additional Steps to Harden AppLocker**
  As with any security measure, there are ways of bypassing AppLocker. Learn how to create rules to mitigate that risk.

APPLY LEAST PRIVILEGES & ACCESS CONTROLS

- ☐ **Exercise Least Privilege**
  As best practice, users should be given the bare minimum of access and privileges necessary, limiting the damage they can do if compromised. Microsoft's Just Enough Administration can help.
- ☐ **When Possible, Use Highest UAC Enforcement Level**
  That includes setting UAC to "always notify," which will trigger prompts whenever a program attempts to make changes to Windows settings or the machine (yes, this can be annoying).
- ☐ **Enable Admin Approval Mode**
  It enforces UAC for the built-in Administrator, which can help thwart privilege escalation and lateral movement attempts.
- ☐ **Remove Users from the Local Administrators Group**
  This can also help prevent privilege escalation attempts.
- ☐ **Disable Credential Caching**
  Don't allow storage of credentials for network authentication. Anytime credentials are stored it presents attackers with an opportunity to grab them.

2018 Cybersecurity Checklist

APPLY LEAST PRIVILEGES & ACCESS CONTROLS (CONTINUED)

- ☐ **Avoid Credential Overlap Across systems**
  This can help prevent lateral movement opportunities if valid credentials are obtained.
- ☐ **Avoid Staying Logged In On Remote Systems**
  Otherwise you open yourself up to attackers hijacking your admin access and privileges.
- ☐ **Disable Anonymous Login for Read and Write Access to Network File Shares (NFS)**
  Open shares provide a pivot point or means to further further spread an attack to other users on the network.
- ☐ **Disable Anonymous Login for Read and Write Access to File Transfer Protocol (FTP):**
  For the same reasons stated above for NFS.
- ☐ **Use Strong Passwords**
  Should go without saying, but obviously still a major common problem.
- ☐ **Utilize 2FA When Possible**
  Requiring two factor authentication can help keep attackers out even if they've successfully stolen passwords.
- ☐ **Apply Account Lockout Policies and/or Progressive Delays for Logins**
  This can help thwart brute force attempts.

MONITOR FOR...

- ☐ **Changes In The Registry**
  Hiding scripts in the registry is one of the most common ways attackers gain persistence. Using WMI subscription events and/or tools like Sysinternals Autoruns can help.
- ☐ **Suspicious WMI Activity**
  Again, creating defensive WMI subscription events (examples here and here) can help.
- ☐ **Scheduled Task Creation**
  Scheduled tasks can be used to achieve persistence and escalate privileges. Track creation with PowerShell scripts.
- ☐ **Suspicious Processes and API Calls**
  Monitoring for specific calls in the PowerShell operational log can provide strong indication of attacks. Using tools like Sysinternals Process Explorer and Get-InjectedThreads can also help.
- ☐ **Processes Being Spawned with the CREATE_SUSPENDED flag**
  This is a good indication of process hollowing.