Security Exploits Lock It Down Checklist

Is Your Company Protected from Security Exploits?

Initial Compromised Prevention – low hanging fruit

The role as protector of the network is to keep attackers from gaining access. If they cannot get on a computer system, website or network device then you have a better chance at defending your business.

☐ **Patch What You Can On Your Network Devices**

Having a system in place to examine, test, and roll out patches is a required first defense against security attacks.

☐ **Identify and Separate What Cannot be Patched**

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

☐ **Secure Remote Desktop (RDP)**

RDP ports exposed to the Internet are weak points to be exploited by attackers. Restrict access to RDP listening ports by placing them behind a firewall

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

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

☐ **Block Malicious File Attachments**

The obvious file attachments (.EXE, .BAT), also consider blocking script files (.JS, .VBS), archive files (.ZIP, .SFX, .7z) can contain malicious files. Office files (.DOC, .DOCX, etc.) and PDFs require extra scanning before sending to a recipient.

☐ **Win-Win with User Awareness Training**

Most attacks still occur when users click something they should avoid. Train and inform your end-users about attacks that start with deception.

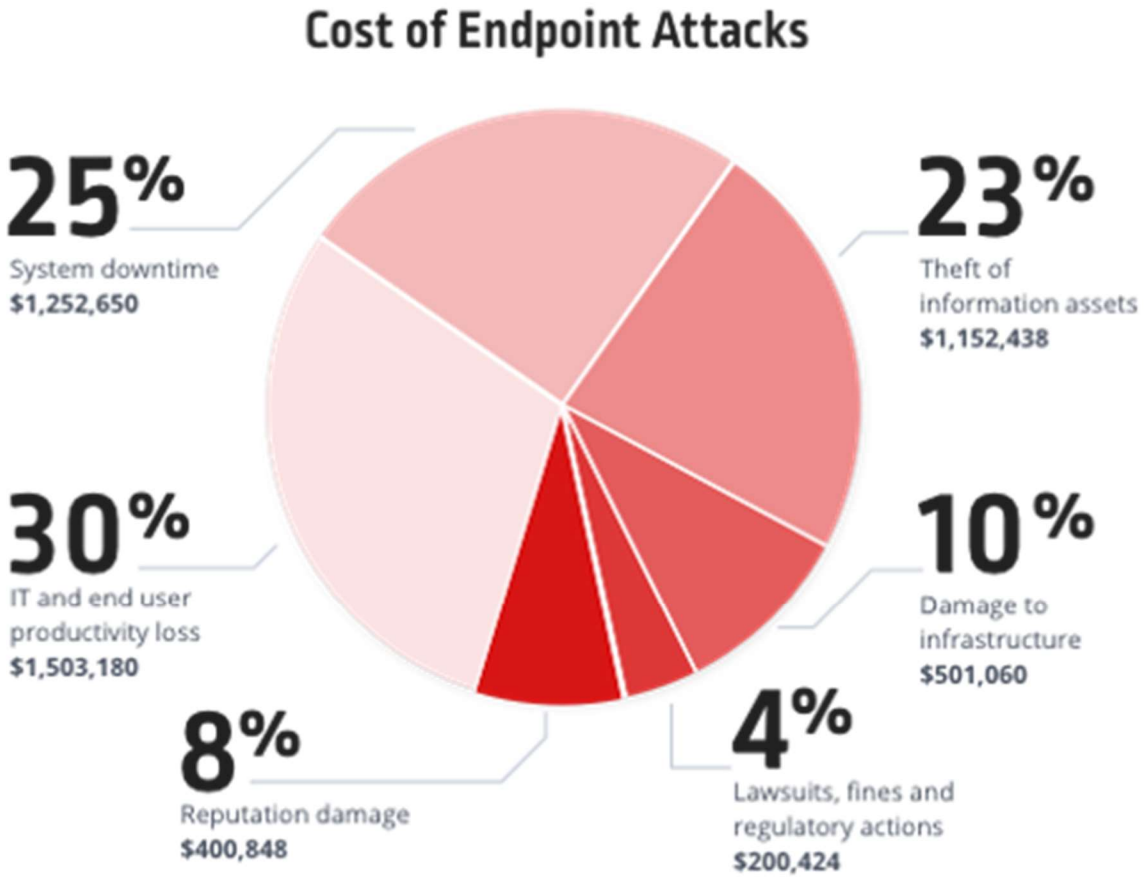
☐ **Utilize Ad-Blockers**

Legitimate websites can serve as infection points thanks to malware found in advertising. Malvertising is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

Key Findings from the Ponemon Institute's annual State of the Endpoint Risk Report

For 5 consecutive years, the annual State of the Endpoint Risk Report, conducted by Ponemon Institute, has surveyed IT and security leaders involved in securing endpoints. The 2017 report reveals endpoint security risk is higher and has been found to be more costly than in previous years.

- 54% of organizations reported they were compromised by attacks in 2017
- 77% of successful attacks were either fileless or exploits techniques. All of them bypassed existing endpoint security solutions.
- The average organization lost $301 dollars per employee due to things like system downtime, reputation damage, productivity and data loss.



Initial Compromised Prevention continued – harder to implement
Mitigating techniques used to deter access to the network devices used in your company. Once attackers have access to a machine, they can evade detection by using system administration tools .

- ☐ **Enforce Strict Macro Controls**

Microsoft Office allows file downloads from the Internet usually by using a Macro.

- ☐ **Disable in Microsoft Word**

Disabling "Update Automatic Links at Open"on older Word installs. Choose Options from the Tools menu. Word displays the Options dialog box. Make sure the General tab is selected. Set the Update Automatic Links At Open check box as you desire. Click OK.

- ☐ **Disable OLE Packages**

Microsoft's object linking and embedding feature should be disabled. Microsoft Windows Security blog has great visuals to understand OLE.

- ☐ **Powershell**

Disable it if you can. System Administrators use this scripting tool to gather all sorts of network activity. Update to the latest version if you choose to continue to use Powershell.

- ☐ **Use Highest UAC Enforcement Level**

Setting UAC to "always notify" with the annoying trigger prompts whenever a program attempts to make changes to windows settings or the device. Enable the built-in Administrator approval mode to stop privilege escalation.

- ☐ **Remove Users from the Local Administrators Group**

When you perform the removal of the user from the administrators group it will prevent escalation attempts on the Windows machine.

- ☐ **Use Strong Passwords**

We should be past this but users still manage entirely to many passwords.

- ☐ **Apply Account Lockout Policies**

Brute force attempts are still being used because it is a set it and forget it tool.

- ☐ **Scheduled Tasks**

Ironically we use Powershell scripts to monitor Scheduled Task activities.