Article

Avecto

Guide to the recommendations of the Australian DoD

In this short guide, we review the top four mitigation strategies identified by the Australian Department of Defense as essential for over-coming cyber threats, with practical advice on how to best implement these mitigation techniques.

Introduction

The Australian Government's Defence Signals Directorate (DSD), also known as the Australian Signals Directorate (ASD), maintains a highly regarded strategy paper providing advice to defend against cyber attacks.

The list of 35 Strategies to Mitigate Targeted Cyber Intrusions is informed by the ASD's experience in operational cyber security. This includes responding to serious cyber incidents, performing vulnerability assessments and penetration testing for Australian government agencies.

This guide is one of the first security advisories developed using real-world attack data from public and private organizations.

The top 4 essential mitigation strategies

01 Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.

02 Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.

03 Patch operating system vulnerabilities. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.

04 Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.

The top 4 strategies should first be implemented on workstations of users who are most likely to be at risk, and then on all workstations and servers.

Avecto

Application control

Downloading and running unapproved software is one of the most common ways that devices are compromised. Anti-virus suites can block applications based on publically available reputational data and heuristics, but as noted in the report, this type of protection is good, appearing at #30, compared with the essential rating assigned to the top 4 mitigation strategies.

How Defendpoint can help

Defendpoint allows administrators to use a common set of rules so users can only run and install trusted applications.

Patch applications and operating system vulnerabilities

Operating system hotfixes and updates can be managed using Microsoft's free Windows Server Update Services (WSUS) role on Windows Server. There are also reporting features so you can check that devices are being updated. Migrating to Windows 8 is beneficial in that one of the most commonly exploited applications, Adobe Flash Player, is integrated into Internet Explorer 11 and updated automatically via Windows Update.

Third-party applications often have their own automated patching mechanisms, but some require users to manually install updates and provide consent using an administrative account, forcing IT to choose between removing administrative rights and allowing users to update applications as needed.

How Defendpoint can help

IT can distribute update packages for third-party applications and use a privilege management solution, in conjunction with application control, to allow standard users to launch approved packages with administrative privileges when there is no automated update mechanism in place.

Restrict administrative privileges

Removing administrative rights from end users is a vital step in ensuring that PCs and servers cannot be compromised with root privileges, which would allow a hacker to completely 'own' the device and data. Preventing unknown processes from running with administrative privileges limits the damage that can be done should a PC be compromised.

Microsoft's built-in User Account Control (UAC) requires standard users to have a separate administrative account to perform privileged tasks, adding an extra administrative burden and limited control over security.

How Defendpoint can help

Defendpoint provides enterprises with an effective solution to ensure minimum impact for end users. It allows them to carry out their job functions and approved computer configuration tasks, and provides an effective security solution with low maintenance overheads and implementation costs, but with a higher return on investment compared to more traditional security products.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.