Avecto

Latest not always greatest

In the era of next-gen technology it's the often-forgotten basics that provide the best foundations.

The 2016 Microsoft Vulnerabilities Report from Avecto provides an important reminder to organizations that we cannot ignore the simple things.

It's a common perception that migrating to the latest operating system will improve security, but in isolation this is not enough to reduce the risk of attack.

Despite Microsoft stating it's "designed to be the most secure Windows ever", Windows 10 had the highest proportion of vulnerabilities (395) compared to any other OS.

And it's a similar story with Microsoft Edge. This is Microsoft's newest and supposedly "safer" browser, yet there were 111 vulnerabilities in 2016. Admittedly, the various versions of Internet Explorer only fared slightly better with a total of 109 vulnerabilities but it will probably still surprise many to learn that Edge is a bigger security issue for those not employing least privilege.

The good news? Removing admin rights could mitigate the risk associated with 100% of these vulnerabilities across both Microsoft browsers.

Microsoft MVP and ethical hacker Sami Laiho agrees with this approach: "The only way to block system wide access to malware is to prevent yourself from accidentally doing it - this is achieved only by limiting the use of administrative accounts.

"Reactive solutions like anti-malware or blacklisting are both technically and mathematically impossible to work anymore.

They have to add 300,000 new lines to their ruleset, while proactive solutions like whitelisting only require approximately one addition per month. I would go for whitelisting."

And our report provided plenty more compelling reasons for doing so. Not least that 94% of critical Microsoft Vulnerabilities can be mitigated by removing admin rights, up from 85% last year.

There were 530 vulnerabilities in total last year, 189 of these were critical. By comparison, take a look back to 2013, the year of our first report, and we saw 325 vulnerabilities, 147 of which were critical.

The benefits of removing admin rights should be clear. However, for some, the reluctance to introduce least privilege across a corporation will be down to the perceived to be difficult of doing so, as well as a belief that it will put up barriers and impact the productivity of the end user.

How to achieve security and freedom

Removing admin rights is just the start of the journey. Removing privileges without a solution in place to ensure employees can continue to be productive creates an over-locked environment which will only drive calls to the IT helpdesk. This situation often leads to 'privilege creep', as admin rights are slowly reintroduced and 'shadow IT' workarounds come into play. It's therefore essential to have technology in place to manage user requests and exceptions.

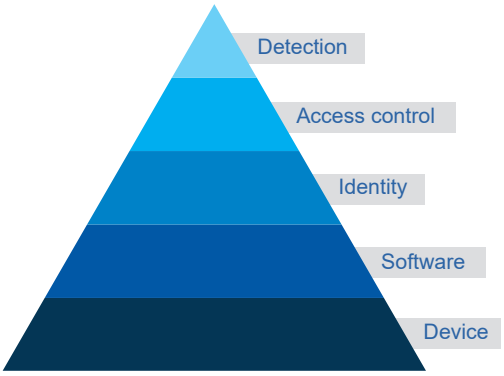
Additionally, malware can still do damage to a standard user account – although there's a much lower risk of widespread data loss. The malware still has access to everything that the user does on the machine.

Avecto

Where to start and how to build up layers of defense

The hierarchy of cyber needs

Microsoft's Hierarchy of Cyber Needs is a clear demonstration of the need to prioritize the different layers of security solutions. It shows how to work up from the device through to software and user access, adding detection as a last line of defense.



Software management needs

Make sure software is licensed and patches are up to date. Failing to do this will limit your ability to protect yourself and leave your computers vulnerable to exploits easily downloaded from the internet.

Identity management needs

You wouldn't run a bank without asking customers for identification when making withdrawals, so don't try to run your business without identity management. Security is easier with privilege management and everyone is able to get on with their jobs.

Access control needs

To avoid putting the crown jewels at risk, the advice is simple - use least privilege to make all users non admin. Least privilege makes critical resources harder to be breached.

Detection

Detection has an important role to play, but can't be relied upon on its own. Importantly, getting applications and content under control first means that detection solutions are not flooded with the same volume of unknown threats.

Defendpoint makes it possible

Remove privileges and remove threats.

Defendpoint's privilege management capability allows you to remove admin rights from all users, to stop attackers from exploiting privileges and gaining access to your data, without harming productivity.

The powerful combination of privilege management and application control makes whitelisting simple - trusted applications and tasks are automatically allowed without the overhead of maintaining long lists, and those that need admin rights are assigned privileges directly. Users never need an administrator account, and unknown code never gets to run.

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.