Avecto

5 reasons why you need to remove admin rights

Time and time again we see large-scale breaches taking place that would have been completely mitigated through the removal of admin rights. Yet, seemingly for the sake of ease and access, many organizations continue to grant a large majority of their employees full administrator privileges.

In this piece we cover why removing admin rights is crucial to your security plans, why it isn't so hard to do, and how it can be done without hindering productivity.

Admin rights overview

As greater emphasis is placed on complying with industry and government regulations, securing data as it passes through personal computer systems is crucial to satisfy auditors and protect systems against data loss and reputational damage.

One major step in such process is the removal of admin rights (to achieve least privilege) in your organization. Such a step is deemed security best practice by many auditors, and means that your business carries much lower risk when it comes to malware and phishing attacks.

> *88% of all Critical Microsoft vulnerabilities since 2013 could have been mitigated simply by removing admin rights.*

Since Microsoft state in their own Security Policy that 'users in the local admin group can manage a computer 100%', we want to help you to understand how you can achieve least privilege, and (in the words of Sami Laiho) why removing admin rights is a proactive measure that should be the first big tick in your cybersecurity plans.

Below are five fundamental reasons on why removing admin rights from your PCs will make your company more secure, followed by the necessary steps to take to reach each solution. Achieving least privilege is now much quicker than you think.

To avoid fines and become compliant

There's lots of talk around the fast approaching GDPR deadline, which will ensure companies either achieve mandatory compliance or face hefty fines. Since the idea of hefty fines isn't so appealing, many companies are already in heavy preparation for May 25.

When an organization doesn't remove admin rights, their users have access to system settings. If they change any of these (intentionally or unintentionally), this can affect your organization's compliance to regulatory standards. And failure to meet these standards means more audits, remediation work and overall cost to business.

Then there is license compliance. If a user has full control over what is installed on their machines (ie. They have full administrator rights), then there is nothing stopping them from using unlicensed software. This then provides a gateway for cyberattacks and hackers – who are more than willing to capitalise on an innocent mistake, which could inadvertently cost your company lots of money.

Least privilege and app whitelisting are very common in most of the mandates so it makes sense to start there and get the foundations right first. With the launch of Avecto's new Quick Start policy, it is now possible to achieve least privilege overnight, removing admin rights from your organization and getting you on the right tracks to achieving compliance.

To keep malware off your computer

If malware infects a user with admin rights, it can cause incredible damage locally, as well as on a wider network. We've seen this firsthand with the WannaCry ransomware virus that hit the NHS back in May 2017. 19,500 medical appointments were cancelled, computers at 600 GP surgeries were locked and five hospitals had to divert ambulances elsewhere (according to the National Audit Office).

Additionally, employees with admin rights have access to install, modify and delete software and files as well as change system settings.

> *As your computer can't differentiate between good and bad software, the only way to prevent the installation of malware is to prevent installations as a whole.*
>
> **Sami Laiho**

Most malware can only do as much damage as the active user is permitted to do, and malware that infects standards users (non-admins) can't install, alter or delete other software packages. In other words, limiting your own abilities also limits what malware can do.

Learn how Defendpoint can stop untrusted applications from running so that malware can't execute, before applying a higher level of protection to those you do trust with TAP (Trusted App Protection).

Defendpoint's application control and privilege management capabilities allow only trusted applications to run, blocking ransomware payloads from executing.

To prevent zero-day attacks

Zero day attacks exploit software or hardware vulnerabilities where there is no prior knowledge of the flaw. The attack occurs in the time between the vulnerability being discovered, and a patch being applied.

Running with reduced privileges can mitigate a majority of software vulnerabilities in Microsoft, Adobe, and a number of other operating systems.

Any vulnerability has the potential to be a zero-day. Running software with reduced privileges protects against threats that could be lying within commonly used software during this period.

> *An ever-increasing amount of new code and a robust underworld economy will be stoking the market in 2017 for zero-day vulnerabilities.*
>
> **John p. Mello, Jr.**

Learn more on this subject via our zero-day timebomb infographic, and learn how Defendpoint takes a proactive approach in mitigating the threat entirely.

To keep your PCs clean

The very idea of privilege management is that everyone operates as a standard user. In a least privilege environment, it isn't possible to write files or make entries in the places that admins can.

"This creates a trickle-down-effect that benefits the whole IT system" says Sami Laiho, "including faster-responding software and more efficient computers."

"This translates into fewer OS re-installations and therefore, less help-desk impact. Ultimately, businesses will give their PCs a longer lifespan."

To be more prepared for the future

If there's ever been a year in which cybersecurity has taken the headlines, it's 2017.

With huge organizations such as the NHS (WannaCry attack), and more recently Uber, falling victim to high profile cyber-attacks – compromising millions of people's sensitive data – the world is becoming increasingly aware of the importance of cybersecurity.

On top of these attacks there was also the fast and wide spreading Petya ransomware virus, which affected thousands of organizations across the globe. The fact that this took place within two months of the NHS WannaCry outbreak meant that more companies sat up to take notice.

What came to light after these major attacks happened, is that removing admin rights would have stopped both from spreading.

Removing admin rights and achieving least privilege is the best first step any organization can take if they want to take more control of their online security. And it's not even as hard as you might think. Get in touch today to discover more about Defendpoint, or watch our free demo to understand how we can help you achieve least privilege in a matter of hours.