The One Big Thing You Can Do To Mitigate Cyber Attack

Today's external cyber threats are more sophisticated than ever, with advanced next generation attacks continuing to pose a threat to organizations across the globe. This article reveals the One Big Thing you can do today, to immediately mitigate the threat of cyber attack.

The challenge: Understanding today's threat landscape

Today's external cyber threats are more sophisticated than ever, with advanced next generation attacks continuing to pose a threat to organizations across the globe. Without appropriate security measures in place, companies are facing the risk of data breaches, loss of employee productivity, damage to brand reputation and non-compliance, leading to potentially severe fines.

External threats

Malware is constantly evolving, with millions of forms of malware being released every year. In fact, McAfee catalogs over 100,000 new malware samples a day (69 per minute)[1]. With that, successful cyber-attacks have risen 20 percent year on year, with the average cost of cybercrime standing at over $7m dollars a year[2].

Insider threats

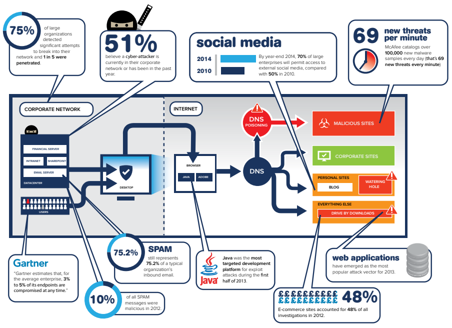
Increasingly, threats faced by enterprises are coming from the inside as well as the outside. The headlines in 2013 and early 2014 have been dominated by stories of data theft driven by rogue insiders. Details of the most high profile event of all, the notorious breach by Edward Snowden at the NSA, continue to emerge almost a year later.

With research commissioned by the UK BIS finding that 84% of data breach incidents are caused by staff, business leaders must be prepared for the risks associated by insiders gaining access to corporate information.

According to a recent report, more than 80% of business users use cloud applications without the knowledge or support of corporate IT[5].

Cyber security predictions

Analysts and industry experts predict that cyber-attacks will continue to evolve in 2014 and beyond, with attackers becoming more sophisticated in their efforts to find holes and vulnerabilities into the operating system and corporate network. To protect your organization, constant vigilance is required in ever shifting attack vectors.



75% of large organizations detected significant attempts to break into their network and 1 in 5 were penetrated.

51% believe a cyber-attacker is currently in their corporate network or has been in the past year.

By year-end 2014, 70% of large enterprises will permit access to external social media, compared with 50% in 2010.

McAfee catalogs over 100,000 new malware samples every day (that's 69 new threats every minute)

"Gartner estimates that, for the average enterprise, 3% to 5% of its endpoints are compromised at any time."

75.2% SPAM still represents 75.2% of a typical organization's inbound email.

10% of all SPAM messages were malicious in 2012.

Java was the most targeted development platform for exploit attacks during the first half of 2013.

web applications have emerged as the most popular attack vector for 2013.

E-commerce sites accounted for 48% of all investigations in 2012.

Infographic: The Evolving Malware Landscape

McAfee: "In the spy vs. spy world of cybercrime and cyberwarfare, criminal gangs and state actors will deploy new stealth attacks that will be harder than ever to identify and stop." McAfee Labs 2014 Threat Predictions

Gartner: "We are in one of those periods that occurs every five years or so, where the attackers find new levels of vulnerabilities to exploit, and the threats get ahead of the standard level of protection." Gartner, Strategies for Dealing with Advanced Targeted Attacks.

The solution: The One Big Thing you can do today

The solution to improving your defenses against cyber threats can be directly attributed to the removal of local admin accounts.

Removing admin rights from all users, you immediately improve your security posture, mitigating 96% of Windows vulnerabilities[3] and much more. Malware and hackers actively seek out users with admin rights to enable the access they need to files, data and the central network where they can inflict the most damage.

Ethical hacker Sami Laiho, a renowned Microsoft MVP, commented in a recent blog post: “All big zero-day attacks reported in the media from 2010-2013 required admin rights! Malware could never affect the computer in the first place without admin rights.”

Neil MacDonald, Analyst at Gartner described how “The single most important thing you can do to improve endpoint security is to remove admin rights from Windows end users”.[4]

Government recommendations

10 Steps to Cyber Security – published by GCHQ, BIS and CPNI

The UK Government provides advice for helping businesses minimize the risks to company assets, stating that c.80% of known attacks would be defeated by embedding basic information security practices in 10 key areas, including Managing User Privileges, Monitoring and Malware Protection, amongst others.

“Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.”
— 10 Steps to Cyber Security

Australian DoD - Top 35 Strategies to Mitigate Targeted Cyber Intrusion

Based on research of attack techniques carried out in 2010 and updated in 2014, the Australian DoD concluded that 85 percent of cyber-attacks could have been prevented if its top four recommendations had been followed:

- ✓ Use application whitelisting.
- ✓ Patch applications.
- ✓ Patch operating system vulnerabilities.
- ✓ Minimize the number of users with administrative privileges.

“In a properly designed, administered and maintained environment there is no requirement for any user to have administrative privileges on their day-to-day account.” Australian Department of Defense.

Implementing least privilege

All organizations are facing an impossible compromise. The challenge is in finding the right balance between organizational security and user freedom. Remove admin rights and the organization immediately becomes more secure, but the employees find themselves unable to function efficiently in their day to day roles, causing frustration for the user and increasing strain on the IT helpdesk. Grant admin rights and you immediately open up the enterprise to a range of internal and external attacks.

To effectively protect the endpoint, elevated privileges must be removed. The principle of least privilege, where all users operate with the minimum privileges they require, is achievable – as long as you have the right tools in place to enable the effective management of privileges across the enterprise.

Summary

Removal of admin rights is the one big thing you can do today to immediately mitigate the impact of cyber threats. Effectively managing user privileges is the key to creating and maintaining a clean operating system, empowering users and securing your business environment.

Any approach to remove admin rights should not be taken lightly and must be strategically planned. Avecto always recommends that businesses start with an admin rights audit to determine the users and apps running with admin rights across the desktop and server estate.

> “ The single most important thing you can do to improve endpoint security is to remove admin rights from Windows end users. ”
>
> Neil MacDonald, Gartner

A layered security approach, using proactive internal and external measures such as application whitelisting and privilege management should be coupled with reactive defenses such as antivirus, to ensure the most robust protection.

About Avecto Privilege Guard

Standard Windows tools such as UAC do not provide the flexibility required to effectively manage privileges, with an ‘all or nothing’ approach leaving users severely restricted.

A privilege management solution such as Privilege Guard allows organizations to find the elusive balance, by removing admin privileges from the end users and instead assigning them to the applications, tasks, processes and scripts that require them. This allows all users to effectively function with standard user rights, while providing customized messages allowing users to quickly and efficiently gain access to files and apps they need – without the associated security risks.

Comprehensive reporting and auditing tools provide a clear view of the number of admin users in the business, and apps that require admin rights to run, so that intelligent policies can be created and maintained.

Sources

[1] McAfee Infographic: State of Malware
[2] Ponemon Cost of Cybercrime Report 2013
[3] 2013 Microsoft Vulnerabilities Report, published by Avecto
[4] Webinar, Best Practices For Removing End-User Admin Rights On Windows
[5] McAfee Labs 2014 Threat Predictions