Avecto eBook

C-level guide to defense in depth

Chapter 2: The hidden flaws in Windows

Sami Laiho, MVP Windows Expert

Contents

Synopsis

In just a few years, the security threats out in the wild have changed dramatically and the amount of them has grown exponentially. We've seen the major anti-malware companies and their executives publicly declare the usage of reactive measures to be insufficient to protect PC's in the future. Why? The reasoning behind this is quite simple actually.

As reactive security measures aims to identify the 200,000 new samples gathered every single day in 2014*, the ever increasing volume makes this a seemingly impossible task. On the other hand, proactive security only needs to identify a few hundred applications trusted by a company.

In this chapter, ethical hacker and Microsoft MVP Sami Laiho will focus on the Windows platform and explore the hidden flaws in Windows that make proactive security solutions the only way forward for 2015 and beyond.

*Source: Pandalabs annual report 2014

About the author

Sami Laiho

Sami Laiho has been a MVP Windows Expert - IT Pro since 2011 and is part of the Microsoft STEP community. He has been training and consulting on everything in connection with the Windows OS for 20 years.

Sami Laiho has also been a Microsoft Certified Trainer for over 15 years. Sami's speaking session was evaluated as the best session in TechEd North America 2014, TechEd Europe 2014 and TechEd Australia 2013.

The hidden flaws in Windows

Windows' security subsystem works like an onion model, with many different layers. We can't forget the most important layer of educating users and having good written instructions, training and security policies – as social engineering is still the most difficult form of attack to protect against.

All other layers can be technically hardened and configured for different levels of security though– it's the human factor which remains mostly out of our control.

The foundation of Windows' security subsystem relies on a few basic rules:

01 Administrative users cannot be controlled by design and therefore all other security measures will be vulnerable if a user has administrative access to his or her operating system

02 You cannot build a secure Windows-installation without restricted physical access or hard drive encryption

These are the strongest laws of security for Windows so we'll start with these two topics and the dive into other solutions that can be implemented if these are taken care of properly.

For a laptop computer without tight physical security, you need to have both of the above in place as the lack of hard drive encryption actually leads to a situation where administrative access to a box can

be achieved with a single command – as I've presented in numerous different conferences.

Getting rid of administrative rights in Windows

The problem with the Windows' security model is that the only way to configure it with built-in tools is to either give administrative access to a single computer or a single user. As users need to have enough access to perform their jobs without problems, this needs to be changed to work in a way where you can give administrative access to a single process in an operating system, for example for changing a static IP address or running a business-critical application. Although the Windows operating system offers API's to do this there is no way to do it without 3rd party tools like Defendpoint from Avecto. Common problems that arise from users being given administrative access are:

- Ability to block company policies from applying to a user or computer
- Administrators can't be controlled by access control lists because in Windows administrators get superpowers called Privileges that can bypass all ACL-check.
- Ability to turn off protections like encryption, network uthentication, firewalls or software whitelist
- Local administrative users can decide what is run on the computer when any logs on. This leads to a problem where the helpdesk personnel can be easily lured to run commands with even more powerful user accounts like Domain Admins.

An extra measure you also need make sure is in order is the policy that forces your Domain Admins to have at least three user accounts:

01 A user account for daily use like reading email and surfing the web
02 A user account that has administrative access to workstations and possibly member servers
03 A user account belonging to the Domain Admins group for administering the Active Directory environment

Implementing hard drive encryption in Windows

In Windows, I always recommend to use the built-in BitLocker encryption. You need to have an Enterprise-version of Windows 7 or any version of Windows 8 or Windows 10 to be able to use it. The problem that I mostly face is people calling me and asking me to come and help them implement BitLocker in their environment. I always reply “you’re too late” as an easy to administer, cost-effective to implement and secure BitLocker implementation starts by choosing the right PC hardware.

My number one instruction on this matter is: Never choose laptop models with PCI-Express, Firewire or ThunderBolt connections. All of them support Direct Memory Access (DMA) which is the biggest enemy of any encryption or security technology.

When implementing BitLocker, aim for TPM-only scenario described by Microsoft. That’s perfect for 95% of customers if deployed correctly and it’s both secure and easy to manage.

Remember: if you don't have hard drive encryption on your Windows box, it gets hacked with a single command that can't be prevented by any anti-malware solution out there.

Adding the rest of the needed security measures to your environment

Once you have removed administrative rights for your end users and deployed hard drive encryption, you can start to add the next needed technologies to secure your environment.

To achieve a secure environment, the next most important proactive measure is whitelisting your trusted applications. Before Windows 10, the number one inbox technology is AppLocker but it requires an Enterprise version of Windows.

My number one tip for successful whitelisting implementation is to stop whenever you find yourself adding a single application to your whitelist.

You should always create rules on a container basis with either using folders or publishers – never use hashes or files unless you really know you need to.

The drawbacks of AppLocker

In a Windows environment, the whitelisting has gotten better in every Windows version. Windows NT4 had the ability to list the names of allowed applications. Windows XP added Software Restriction

Policies that could allow applications by path, hash or internet zone. Windows 7 Enterprise includes the most used whitelisting feature nowadays called AppLocker (internally called Software Restriction Policy V2) that allowed the ease of using certificates for allowing applications signed by a trusted party.

The biggest problem with AppLocker is impossible Microsoft to solve really as it's the lack of will from 3rd party application developers to get their code signed. This problem is taken care of in the future Windows 10 by using a more secure "AppLocker" called Device Guard and a signing service provided by Microsoft that will sign applications from 3rd party providers as well.

Windows AppLocker has a few weaknesses in it sadly. One weakness is actually in the OS itself, as Windows requires default rules to allow everything to be allowed from the Windows—and Program Files—folders.

As long as you don't have administrative access those folders should be write-protected, but sadly that's not exactly the case. You need to audit your installation with tools like AccessChk.exe from Sysinternals to find the few subfolders that need to be excluded from your AppLocker rules.

The other weakness is the monitoring of DLL-files. DLL-files are libraries of functions that can do whatever by default if an attacker so wants. These functions can be called by rundll32.exe which is needed by Windows and can't really be blocked.

You can turn on DLL-monitoring in AppLocker but the impact on performance is often too much – test it out yourself as it depends on the environment it is used in.

Defendpoint's Application Control module can be used to make the whitelisting much easier to manage and more secure without affecting the performance. I use it a lot and I like it because I can use it with customers that don't have the Enterprise version of Windows 7 or 8.1 as well.

Summary

Security is always a tradeoff between security, usability and cost. You can always get two but never three. Now it's up to you to choose if you're willing to choose more maintenance and lower user satisfaction, lower security or a higher price tag.

Just remember that proactive is the only way you should go.

About Avecto

Deloitte.
Technology Fast50
UK 2013

Microsoft
GOLD CERTIFIED
Partner

Avecto is a global software company specializing in endpoint security. Its revolutionary Defendpoint software offers proactive protection against advanced threats. Uniquely combining the technologies of Privilege Management, Application Control and Sandboxing in an integrated suite, you achieve security strength and depth without compromising user experience. This mantra of security + freedom underpins Avecto's philosophy to unite IT departments and their end users.

Avecto's experience is proven, with implementations of over 5 million endpoints at many of the world's most recognizable brands. Established in 2008, Avecto is headquartered in Manchester (UK) with offices in Boston, (US) and Melbourne, (Australia).

Contact

Avecto
@avecto
+Avecto

avecto.com
info@avecto.com

UK

Hobart House
Cheadle Royal Business Park, Cheadle, Cheshire, SK8 3SR

Phone
+44 (0)845 519 0114
Fax
+44 (0)845 519 0115

Americas

125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone
978-703-4169
Fax
978 910 0448

Australia

Level 8
350 Collins Street, Melbourne, Victoria 3000, Australia

Phone
+613 8605 4822
Fax
+613 8601 1180