Global Knowledge™

Expert Reference Series of White Papers

The 10 Most Dangerous Risks to Microsoft Security

1-800-COURSES

www.globalknowledge.com

The 10 Most Dangerous Risks to Microsoft Security

Royce Howard, MCSA, MSCE, MCITP-Server Admin, Enterprise Administrator

Introduction

Security has always been an important part of any IT infrastructure. As technology progresses, it's a safe bet that there will always be people who will try to infiltrate your network to do their malicious deeds. As security technology improves, so do the skills of these notorious hackers. But what can we do to protect ourselves from these threats? This white paper has tips to help improve your awareness of some of the more important risks threatening your Microsoft infrastructure.

1. Physical Attacks

Let's start with the most basic attack. A physical attack on a computer can be a daunting thing. Suppose someone actually has physical access to a machine, and they wish to obtain data from it. With heightened awareness of password security, things are a little better. However a determined hacker can easily get to information that is stored on a machine whether it be a stand-alone client or a full-blown domain controller. Some obvious best practices include making sure that no one has physical access to any of your servers. Hopefully, most organizations running a back-end SAN will have whatever room the servers are located in under lock and key. Physical attacks can also include an attacker coming in with an external hardware device like a usb drive and infiltrating a system that way.

Thankfully, Microsoft has supplied us with group policy settings so we can set a policy in place that prohibits the use of any type of external storage device. With the advent of Microsoft Server 2008, Microsoft has also given us Read Only Domain Controllers (RODC), and this helps tremendously as far as networks are concerned. Because of the unilateral replication, if any of the structure is changed or manipulated, it ensures that the changes won't be replicated out to the rest of the network, not to mention the choice of which account credentials will be cached.

We were also given the new BitLocker feature to help protect sensitive data. BitLocker Drive Encryption is a full disk encryption feature included with Vista Ultimate and Enterprise as well as the new Windows 7 and Server 2008. It's designed to protect data by providing encryption for entire volumes. It uses the AES encryption algorithm in CBC mode with a 128 bit key. However, as with anything else in terms of security, hackers found a work-around.

Back in February of 2008, a straightforward cold boot attack was discovered. This basically allows a machine that is protected by BitLocker to be compromised by booting the machine off of a USB device into another OS and then dumping the contents of the pre-boot memory. The attack relies on the fact that DRAM retains information for up to several minutes after the power has been removed. If cooled, it can buy the attacker even more time. This takes away any protection because the keys are held in memory while Windows is running. BitLocker can also operate in a sort of "USB Key" only mode. Of course, anyone using this method better be sure that the key is never left with the computer. There is also the possibility that a malicious program, like a pre-boot or post-boot malware program, could read the startup key off of the USB key and store it. It's always a good idea to remove the USB key from the USB port before Vista completely starts.

2. Password Policies

When talking about password policies, we often think of complexity requirements. This can include number of characters, type of characters (letters, upper-case, lower-case, numbers, and special characters), how often the password should be changed, and failure threshholds. Any password policies not using Kerberos are using NTLanman, which uses 56-bit DES encryption, and that's really weak. Unless you happen to be running any NT boxes in your network, you can rest easy knowing that Kerberos authentication, with it's Advanced Encryption Standard (AES), is at work for you. However, one thing that can often be overlooked is that any password that is less than 15 characters long is automatically stored in backup with an NTLanman backup hashfile.

Taking this into consideration, it's easy to realize why you might want to have a password policy that requires a password of over 15 characters. So instead of a password, have your users come up with a passphrase instead. You might even consider having your users change the password every 90 days instead of every month because it cuts down on the chance that the user might write down their password. From a security standpoint, any passwords that are written down for someone else to possibly see are a potential hazard.

3. Privileged Accounts and Social Engineering

Let's say that you're the network admin at your organization. You have full domain rights and privileges. You go to install a new vulnerability scanner that your friend Bob recommended to you (so you know it's from a safe source, right?). Unbeknownst to you, the program actually has a series of simple net commands that are running in the background that create a new domain account, change your password, and a few other things that make you cringe in retrospect. How could this have happened? After all, you're certain that your anti-virus software is up to date. The problem with this scenario is that it has nothing to do with a virus. According to the system, it was you who created the new admin account and changed your own password.

Over the years, the game in security has changed from "Can I guess your password?" to "How can I get you to run something while you're signed on with your privileges?" Because of the way that security works within Microsoft, as soon as you login with an account that has administrative privileges, you possess a "token" that gives you access to those privileges. Whether it be establishing rapport and good credibility with Bob and then offering him a new vulnerability scanner to try at work or setting up a web site with dirty active x controls, attackers can get pretty creative in how they try to accomplish this.

Microsoft has been telling us for years not to login with an account with administrative privileges and go web surfing, and checking our e-mail. Hence the "run as" feature that was so kindly given to us. While working with an account with non-admin rights, if we need to install a program, we can right-click and choose "run as" and only that one process will use the administrative token. Windows Vista tried to alleviate much of this by giving us the User Account Control (UAC), but how often is it really used or turned off altogether?

A company called BeyondTrust released a report recently that indicates that according to their analysis of all the security bulletins Microsoft published last year, 92% of the critical vulnerabilities could have been mitigated by the principle of least privilege. Below are some key points from the report.

- 92% of Critical Microsoft vulnerabilities are mitigated by configuring users to operate without administrator rights
- Of the total published Microsoft vulnerabilities 69% are mitigated by removing administrator rights
- By removing administrator rights, companies will be better protected against exploitation of 94% of Microsoft Office, 89% of Internet Explorer, and 53% of Microsoft Windows vulnerabilities
- 87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights

4. E-mail Attacks

Imagine that you've just sat down to check your e-mail, and you receive an e-mail claiming to be from your bank or, better yet, from your HR department, claiming that a new policy is in place and it's required that you change your password for security reasons. You click on the link provided in the e-mail only to be directed to a site that looks alarmingly identical to your bank site or your internal HR site. At the site, it asks you to put in your current credentials for authorization. Spam and phishing attacks are classics in the online criminal's repertoire. But, as long as users keep falling for the tricks, the bad guys will just keep sending on the e-mails. These types of attacks can leave you wide open for some of more popular risks such as...

5. Worms

We've all heard of computer worms. Basically a self-replicating program, they use our networks to send copies of themselves to other machines, and they do so without any intervention on the user's end. It doesn't need to attach itself to an existing program like a virus. Although they don't corrupt or devour files like a virus, worms can still pose a security threat nonetheless, usually in the form of bandwidth consumption.

The Conficker worm that caused so many problems to networks recently is still around. It was so serious that Microsoft thought it was worth putting a $250,000 bounty on the head(s) of those who created it. However, the worm is still out there and spreading. A new variant known as Conficker B++ has been released into the wild sporting new characteristics that could try to get around the IT industry's attempts to bring it down.

6. Increasingly Malicious Malware

Malware is malicious software. We've all heard of malware infecting our systems. We usually only find out about it through scans because they're designed to infiltrate or damage a computer system without the user's consent. Although most of the malware is not malicious in nature and is usually referred to as spyware, the threat of malicious software infiltrating our machines is an ever-alarming one.

Hackers continue to refine the capabilities of malware, expanding on flux technologies in order to obscure their infrastructure, making it even harder to locate their servers. There are also recent variants that are able to detect when someone is investigating activity and then respond with a flooding attack against the investigator. As this kind of thing is becoming more main-stream, it's growing more difficult to make investigations. Some examples also target and dodge anti-virus, anti-spyware, and anti-rootkit tools. So basically, malware is becoming stickier on target machines and more difficult to shut down.

When you look at a list of malware threats you may begin to experience deja vu. You might ask yourself if you've seen the names of some of these processes before. The reason is that the writer of the malicious code is trying to pull a fast one and have disguised the code by giving it a name similar to another harmless, but essential, application. Below is a list of some examples taken from ProcessLibrary.com.

ISASS.EXE

Part of Optix.Pro virus, Isass.exe is registered as the Optix.Pro Trojan that carries in it's payload the ability to disable firewalls and local security protections, and which also contains a backdoor capability, allowing a hacker fairly unrestricted access to the infected PC. This Trojan was developed by someone going by the name of s13az3 who formed part of the (since discontinued) Evil Eye Software crew.

NVCPL.EXE

Part of W32.SpyBot.S Worm Nvcpl.exe is a process that is registered as the W32.SpyBot.S worm (it also seems to be associated with the Yanz.B worm, which may just be another name). It takes advantage of the Windows LSASS vulnerability, which creates a buffer overflow, forcing your computer to shut down. Although not necessarily a particularly destructive piece of malware, it is a nuisance because it will access your e-mail address book and send spam to your contacts.

CRSS.EXE

Part of W32.AGOBOT.GH Crss.exe is a process-forming part of the W32.AGOBOT.GH worm. This spyware worm is distributed via the Internet through e-mail and comes in the form of an e-mail message, in the hope that you open its hostile attachment. The worm has its own SMTP engine, which means it gathers E-mails from your local computer and re-distributes itself. In worst cases, this worm can allow attackers to access your computer, stealing passwords and personal data.

SCVHOST.EXE

Part of W32/Agobot-S virus, the scvhost.exe file is a component of the W32/Agobot-S virus. Another member of the Agobot (aka Gaobot) computer worm family, this Trojan spreads via networks and allows attackers to access your computer from remote locations, stealing passwords, and Internet banking and personal data.

SVHOST.EXE

Part of W32.Mydoom.I@mm Svhost.exe is a process that is associated with the W32.Mydoom.I@mm worm. This worm is distributed as an e-mail message and requires that you open a hostile attachment. Using its own SMTP engine, the Mydoom worm will gather e-mails from your local computer and redistribute itself. The original Mydoom worm was first spotted in January 2004 and went on to become the fastest spreading e-mail worm ever. In worst case scenerios, this worm can allow attackers to access your computer, stealing passwords and personal data; however, it is also interesting in that, in addition to the Trojan, the other payload it carried was a denial of service attack on the website of SCO Group. Later versions of the worm have included denial of service attacks on other sites, including Google and Lycos.

7. Unauthorized Network Access

Probably one of the biggest risks to keep an eye out for would be any type of device that has access to the network that should not. Just imagine a scenario where someone is able to walk into your organization and plug in a wireless router that starts automatically handing out IP addresses. Fortunately, we have tools at our disposal to prevent something like this. These tools include Network Access Control (NAC), which uses a set of protocols to define and implement a security policy that describes how to secure access to network nodes by devices when they initially attempt to access the network. Thus, when a computer connects to a computer network, it is not permitted to access anything unless it complies with a set of standards, including anti-virus protection level, system update level, and configuration. While the computer is being checked by a pre-installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the standard is met, the computer is able to access network resources and the Internet, within the policies defined within the NAC system.

We also have Network Access Protection (NAP), which is used for controlling network access of a computer host based on the system health of the host. With NAP, system administrators of an organization's computer network can define policies for system health requirements. Examples of system health requirements are whether the computer has the most recent operating system updates installed, whether the computer has the latest version of the anti-virus software signature, or whether the computer has a host-based firewall installed and enabled. Connecting or communicating computers have their health status evaluated. Computers that comply with system health requirements have full access to the network. Administrators can configure health policies that make it possible to ensure that computers not in compliance with system health requirements have restricted access to the network.

One of the biggest improvements for ensuring that you're protected against unauthorized use of the network has to be the use of certificate services. Certificate servers validate or certify not only devices on a network but also users and even processes through the use of keys. Of course, the use of managed switches and protocols, like ipsec to help protect data and ipv6, don't hurt either.

8. Not Updating Patches

Of course most of these threats could be avoided altogether if everyone followed best practices and made sure that all of their patches are up to date. For the common end user, it's just a matter of keeping auto-update turned on inside of Windows. For a larger organization, things may not be so simple. Patches and updates have to be tested before being rolled out on an active network to ensure there won't be any conflicts with other software that might be running. Sometimes, the software running may be detrimental to the functioning of the particular organization. Of course, this is where having a testing environment along with Windows Software Update Services can be key. With WSUS, administrators have more direct control over the type and time updates are applied to network systems. This not only controls precious bandwidth but also gives administrators control over yet another entry point into their networks. This might seem obvious, but neglect in this department can be catastrophic as it keeps the door wide open for all the exploits and vulnerabilities set forth by all the viruses, worms, and rootkits that malware and other types of attacks have lying in wait.

9. Third Party Applications

It's fair to say that Microsoft has put tremendous effort into adding a lot of security in the Windows operating system as well as its Microsoft Office applications. It seems that as our operating systems become more secure, attackers are beginning to focus more on application exploits rather than OS exploits. Microsoft is generally great about routinely updating Internet Explorer to patch any security vulnerability. However, the vendors of many third-party applications are less security-minded or aware. Just think of how many independent developers there are out there offering freeware. Some of these programs present an opportunity we can expect hackers to take advantage of because most have not been written with security in mind and do not automatically check for and download security updates.

10. The Human Factor

A lot of the things mentioned here also rely on one of the biggest vulnerabilities in any IT infrastructure whether it be Microsoft or any other platform, the human factor. The weakest link in all security initiatives are the people. When thinking of this, it reminds me of a term we used to use when troubleshooting back in the day. "I know what the problem is. It's PEBKAC" (problem exists between keyboard and chair). Without heightened awareness of things like social engineering, password security, e-mail scams, and best practices, like keeping all of your software updated, all of these things will continue to thwart the normal functioning and security of our systems.

When deciding what the most dangerous risks to any network are, one must try to imagine where the attacks may be coming from and, more importantly, how they will try to get into the network. Becoming familiar with these "holes" and how they're approached is key to protecting our data and ensuring that our systems won't be infiltrated.

As of this writing, there are currently some very specific exploits concerning the server products and other applications such as "token kidnapping." This allows an attacker to gain full control of a server if the attacker can first run malicious code on the server as a lesser privileged user.

There is also an open exploit involving Microsoft PowerPoint. The bug affects PowerPoint 2000, 2002, and 2003, as well as the edition included with Office2004 for Mac. According to Microsoft, the vulnerability is in the way that PowerPoint parses the older file format used by those versions, and can't be used by attackers to run additional malware and hijack the PC. Rest assured, Microsoft will take the appropriate actions to protect their customers, which may include providing a solution through the monthly security update release process, or an out-of-cycle security update. Exploits and vulnerabilities come and go, but as long as best practices are followed, and we stay up to date with our information, we can be confident that we are protected.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course:

Defending Windows Networks

For more information or to register, visit **www.globalknowledge.com** or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Royce Howard is a Microsoft Certified Instructor working out of Jacksonville, Florida. He started in the IT field back in 1997. He has worked for companies such as America Online, Bellsouth, and AT&T. He currently holds the following certifications: MCSA, MSCE, MCITP-Server Administrator, Enterprise Administrator, MCT.