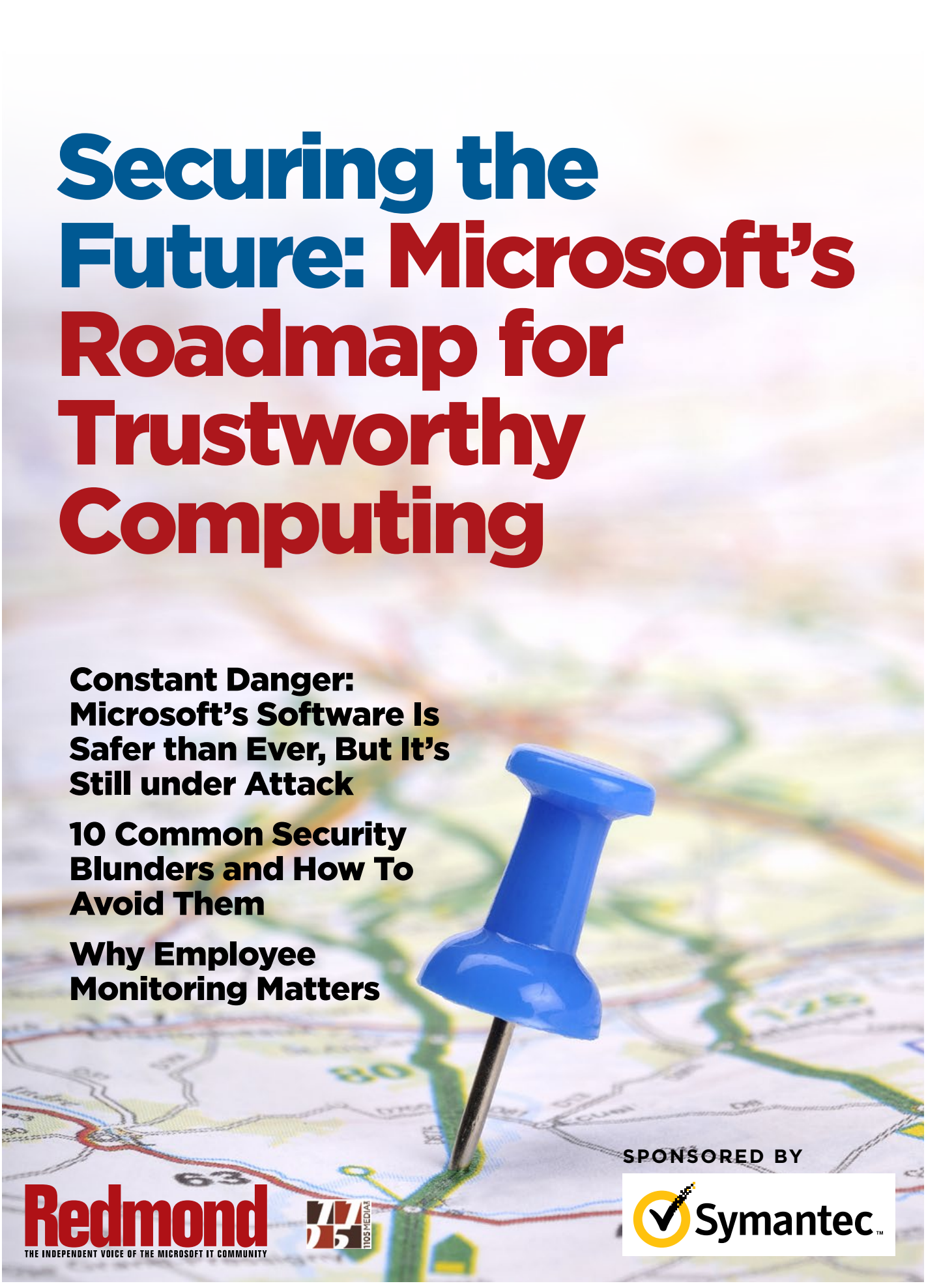
Securing the Future: Microsoft's Roadmap for Trustworthy Computing



Constant Danger: Microsoft's Software Is Safer than Ever, But It's Still under Attack

10 Common Security Blunders and How To Avoid Them

Why Employee Monitoring Matters

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

1105 MEDIA

SPONSORED BY

Symantec™

Symantec Website Security Solutions, Formerly VeriSign SSL Certificates

Symantec Website Security Solutions enable you to protect your website with confidence and accelerate your business growth, knowing you have partnered with the world's leading Certificate Authority. Symantec's industry-leading SSL, certificate management, vulnerability assessment and malware scanning work together to keep your business well ahead of evolving threats. The Norton™ Secured Seal and Seal-in-Search™ assure your customers they are safe from search to browse to buy. Symantec's investment in practices and technologies that consistently up level industry standards means a more secure future for the Internet—and for your business.

Symantec. Confidence in a connected world.

Constant Danger: Microsoft's Software Is Safer than Ever, But It's Still under Attack

A decade after launching its Trustworthy Computing initiative, Microsoft has come a long way but faces new challenges.

By Jeffrey Schwartz

Bill Gates was famous for sending e-mails when he was in command at Microsoft. Most were minutia. Some were game changers such as the message he sent Jan. 15, 2002, pledging to spend the next 10 years making Microsoft products as secure as possible.

Critics scoffed. After all, Microsoft software was a powerful magnet and open target for hackers who spread malicious worms and viruses, and the company was more known for features than lock down. Windows clients and servers, Office, Exchange and SQL Server and all the rest regularly succumbed to vicious attacks. Users and pundits felt Microsoft just didn't do enough about it.

Gates' 10-year deadline has recently passed, and by most accounts Microsoft software today is far more secure and trustworthy. That said, the company remains the No. 1 target of hackers.

Microsoft has done a lot. When it builds software, security is job one. It also releases patches on the now famous Patch Tuesday, more frequently if need be. It has its own free software through Defender and Security Essentials, funds research through its labs, works with keys organizations and third parties, and supports law enforcement.

Law enforcement efforts are paying public dividends. The recent takedown of command and control servers in Scranton, Pa., and Lombard, Ill., set up by a ring spreading the Zeus botnet, is evidence Microsoft software is still a key target, but also that cyber criminals can at least be stymied. But while Microsoft led the FBI to shut down the command and control servers for the fourth time, security experts agree it's only a matter of time before the Zeus botnet or variants resurface.

Experts say Microsoft has made remarkable strides in improving the safety of its software, and many now regard the company as a leader in security-related initiatives. Nonetheless, it faces numerous challenges, such as:

- Increased number of cyber criminals who have more sophisticated skills and can build on the past work of others
- Growth of attack points such as smartphones, tablets and cloud services
- Users who continue to engage in unsafe practices
- The pending release of new client and server platforms including Windows 8 and Windows Server 8.

In assessing Microsoft's progress over the past decade, it's important to recall how terribly insecure its software used to be.

String of Malicious Attacks

Six months before Gates' directive, the Code Red worm wreaked havoc on more than 300,000 hosts running Microsoft IIS. Code Red, which exploited an IIS vulnerability, caused buffer overflows that overwhelmed the memory in the servers. It also unleashed distributed denial of service (DoS) attacks on its targets. Among its notable victims: the server farm running the White House Web site.

Another variant of the worm, Code Red 2, surfaced a month later. Code Red worms were so massive experts worried such attacks threatened the very stability of the Internet. The Code Red worms followed a string of attacks in prior years, including Melissa in 1999, a worm that took advantage of flaws in Microsoft Word and Outlook and erased files. Another one, the ILOVEYOU virus, spread by e-mailing an executable Visual Basic program to the first 50 addresses in a victim's Outlook address book.

The final straw came in 2001, a week after the September 11 attacks, when the Nimda exploit struck. Like Code Red, it also took advantage of vulnerabilities in IIS, and not only was it able to spread itself via e-mail but it also infected files via open network shares and back doors left open from prior worms. Some at the time wondered if Nimda was unleashed by terrorists, a myth that was quickly dispelled.

> "We knew we weren't going to get vulnerabilities down to zero, so we had to think about, 'How do you make a user safe, even if there are vulnerabilities in products?'"

Scott Charney, Corporate VP, Trustworthy Computing, Microsoft

Nimda left Microsoft's reputation at an all-time low as the attacks left some of the world's largest corporations and government agencies hamstrung. "Their software was full of holes from a security standpoint," notes Philippe Courtot, chairman and CEO of Qualys Inc., a provider of malware detection, policy compliance and vulnerability assessment tools.

With so many flaws in Microsoft's software, critics had no faith the company could ever change its stripes. Among those fed up was Alan Levine, chief information security officer at Alcoa Inc., a large industrial provider of aluminum with $23 billion in revenues at the time.

"I made no bones about the fact I thought they were failing in their mission. They were putting out software that contained exploitable vulnerabilities," Levine recalls. "They were causing lots of large companies like mine to go through lots of work and rework and more rework. Every time Microsoft identified a problem, they appeared to be identifying it a day late and a dollar short. And when they issued a patch to fix a vulnerability, it was bad, so they had to come out with a patch to fix the bad patch, which was costly. It left us in a mode where we were less secure."

The Gates Ultimatum

After the September 11 attacks and the Nimda outbreak, Gates knew Microsoft and customers could no longer stand for the status quo. "Computing is already an important part of many people's lives. Within 10 years, it will be an integral and indispensable part of almost everything we do," Gates wrote in his January 2002 memo. "Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing."

No one would say Gates went out on a limb predicting computing would be ubiquitous by now. But few believed Microsoft's software would be dramatically more secure 10 years later, or that the company would be seen as a true leader in security.

"Microsoft's reputation for security was best classified as a laughingstock; their security was simply not respected at all," remembers Jeremiah Grossman, founder and CTO of WhiteHat Security, a Santa Clara, Calif., consulting firm that works with large enterprises to combat Web site attacks.

"Most people were skeptical when the whole notion of Trustworthy Computing came out," recalls Art Coviello, who was CEO of RSA Security Inc. at the time and is now executive chairman of the EMC Corp. division that manages RSA assets. "I remained relatively unconvinced until I saw what they were doing."

Coviello recalls when Gates gave a keynote address at RSA's widely followed annual conference in early 2004. "If anyone ever went into a hostile environment and showed a lot of courage, it was Bill," Coviello says. "He did a very credible job helping people understand what Microsoft was attempting to do. It was at that point that people started to give Microsoft a little bit more of the benefit of the doubt."

When Gates issued his Trustworthy Computing initiative, Microsoft invited Alcoa's Levine and a few dozen other top IT pros to join the Microsoft Security Council, which still gathers in Redmond twice a year. Levine agreed to join but admits he didn't think it would do much. "I was worse than skeptical—I was their worst critic. I thought it was mostly public relations," Levine says, adding he was later surprised at Microsoft's progress. "Over the last 10 years the change has been dramatic, remarkable and unbelievably positive. They took on the really important job of fixing what was wrong."

At RSA's most recent annual conference in San Francisco in February, Scott Charney, Microsoft corporate VP for Trustworthy Computing, said the company had set out to reduce vulnerabilities in code by developing and adopting its Security Development Lifecycle (SDL), a blueprint for the development of all software from cradle to grave to ensure vulnerabilities wouldn't be introduced anywhere along the process.

"We did threat models at design time, and coded and tested to remove vulnerabilities in a systematic way across our products," Charney said in his RSA keynote address. "We knew we weren't going to get vulnerabilities down to zero, so we had to

think about, 'How do you make a user safe, even if there are vulnerabilities in products?' So we started to focus on defense-in-depth and reducing exploitability."

In the ensuing years, Microsoft realized it had to become more granular in addressing security across its entire stack. In 2008 it issued new tools that would help partners and customers build end-to-end trust into software using the principles of the SDL. This new approach of striving to build bug-free code was critical in making Microsoft software impervious to actions that would compromise security, experts say.

"Compilers and developer tools all really changed with regard to pushing developers to create better code," says Philip Lieberman, president and CEO of Lieberman Software Corp., a provider of security and systems management software. "They provided gentle but relentless pressure, saying you should do certain things in your code. And they changed out the libraries, and the insecure versions aren't there anymore."

While many third-party ISVs and partners have utilized the Microsoft SDL tools and best practices, many have not, warns analyst Rich Mogull, CEO of security research and advisory firm Securosis LLC. "Honestly, the biggest issue Microsoft faces is getting all the third-party developers to spend more time not only hardening their code, but fully leveraging the tools Microsoft provides to do that," Mogull says.

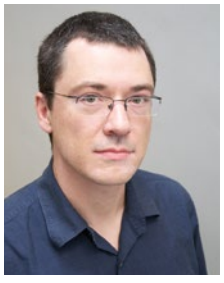
The next big milestones came in 2004, first with the launch of Patch Tuesday: the company's methodical approach to issuing fixes—some critical, some minor—with an eye toward adding predictability around the release of security updates for all of its products on the second Tuesday of each month. The patches come from the Microsoft Security Response Center (MSRC), the company's 24-hour security alerting service. Security vendors and customers have come to rely on the MSRC and Patch Tuesday, and laud Microsoft's emphasis on its approach to providing updates and bulletins.

Another important highlight that year was the release of Windows XP SP2, when Microsoft turned on the firewall by default and likewise turned on auto update by default, enabling the near-touchless installation of patches. The service pack also introduced Data Execution Prevention (DEP), a feature also found in Linux and the Mac OS, designed to protect memory from malicious executable code.

How Windows Vista Changed PC Security

Many think of Windows Vista as a failure because of compatibility problems. But Windows Vista was the first Microsoft OS to implement the SDL, and also introduced several key security features. Among them were PatchGuard, which prevents malware from overwriting the OS kernel; address space layout randomization, which blocks buffer overruns by randomly shuffling the location of code and data in memory to make attacks more difficult to pull off; BitLocker Drive Encryption, which, as the name implies, encrypts data on the drive; Windows Defender, the Microsoft anti-malware scanning program built into the OS (it was also made available as a download for Windows XP); and User Account Control (UAC), requiring user permission before allowing a process that requires administrator privileges.

UAC was not a welcome addition to Windows Vista, as users were constantly badgered by prompts for permission to allow application changes. In Windows 7, Microsoft addressed UAC complaints by extending the tasks that a typical user might conduct without prompting for administrator permission, letting users with admin privileges configure UAC parameters in the Control Panel and offering expanded local security policies that let IT pros reduce UAC messages sent to users.



> "There're plenty of vulnerabilities in Windows 7—it's not perfect software. We'll never have that."
>
> **Chester Wisniewski, Senior Security Advisor, Sophos Inc.**

In addition to a revamped UAC, Windows 7 gained improvements to BitLocker, which extends support for removable drives and offers auditing, and DirectAccess, which allows remote connectivity to enterprise servers and applications without connecting to a virtual private network (VPN). Experts say the encapsulation technique used by DirectAccess offers more secure remote access (see the January 2010 Security Advisor column, "Can DirectAccess Replace Your VPN?" at Redmondmag.com/Wettern0110). DirectAccess, also introduced in Windows Server 2008 R2, uses IPv6-over-IPsec to encrypt communications for secure, remote network sessions.

While Microsoft improved security in Windows Vista and Windows 7, observers point out the client OS still has its share of flaws. "There're plenty of vulnerabilities in Windows 7—it's not perfect software. We'll never have that," says Chester Wisniewski, senior security advisor at Sophos Inc., a provider of enterprise security software and services.

Locking Down Windows 8

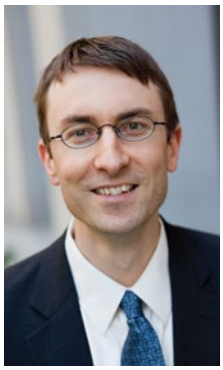
Microsoft is promising the pending arrival of Windows 8 will bring more security improvements. An oft-discussed security feature in Windows 8 is the new version of Windows Defender, the anti-malware tool. Microsoft says Windows Defender added to the new OS will fend off a gamut of malware, bots and rootkits by knowing all of the malware signatures discovered by the Microsoft Malware Protection Center, which will be passed along through Windows Update.

The move by Microsoft to step up the antivirus and anti-malware protection offered with the OS is controversial. Some say it's about time that Microsoft provided better protection for its software, while others are concerned the company is stepping into territory that will cut off third-party security vendors. "Certainly every vendor would like to feel it's on a level playing field, and that we have an equal chance to protect

all of the users with the best possible choices," says Vincent Weafer, senior vice president of the McAfee Labs unit of McAfee Inc., a subsidiary of Intel Corp.

Microsoft is also adding SmartScreen filtering technology to Windows 8. Introduced in Internet Explorer 7, SmartScreen has played a key role in combating social engineering by using what Microsoft calls reputation-based technologies, which can use its cloud-based service to determine the reputation of a URL or app. The addition of SmartScreen to Windows 8 will apply those same principles of assigning reputations to software apps.

> "I don't see any sign of Microsoft coming close to delivering the silver bullet that will solve the security problems the world is struggling with."
>
> **Paul Kocher, President and Chief Scientist, Cryptography Research**



But the Windows 8 security story is more complex. With Windows 8 support for both the new Metro-style interface and the traditional Windows UI, and two hardware platforms (x86/x64 and ARM), there are two new hardware dynamics and two opposing software dynamics.

For example, in the Internet Explorer 10 implementation of Windows 8 running the Metro interface, the browser will not allow plug-ins such as Adobe Flash or Microsoft Silverlight, with the objective of cutting off the chance of malicious code executing.

"Most malware is written to x86, so for ARM they're kind of starting with a clean slate, pardon the pun," Wisniewski says. "There's no existing Windows ARM malware, so that platform will launch malware-free, and obviously Microsoft made additional improvements to the OS itself to be more resilient against attack."

Another feature in Windows 8 aimed at protecting users from attack is AppContainer, which introduces a new security sandbox that Microsoft says offers more fine-grained security permissions and blocks read and write access to most of the system. All of the Metro apps will run in AppContainer.

Vetting App Distribution

It appears Microsoft will require providers of Windows 8 Metro applications to deliver them through the Windows Store, the company's online marketplace. This lets Microsoft make sure applications meet security requirements, much like Apple Inc. does through its iTunes App Store. "If they lock down the way Apple has, I think that can have some dramatic security advantages," Securosis' Mogull says.

"I'll be curious to see if they're as restrictive as Apple, where you can only get software from the market," Wisniewski wonders. "If they do that, they may be able to reduce the amount of crust out there that targets that platform and be able to keep it largely malware-free—at least comparative to the existing Windows environment, where the numbers are huge."

Internet Explorer 10 Gains Enhanced Protected Mode

While the Metro version of Internet Explorer 10 won't allow plug-ins, both versions of the new browser will support a feature called Enhanced Protected Mode.

Enhanced Protected Mode advances Protected Mode, a capability introduced in Internet Explorer 7 that blocks attackers' ability to install software or change system settings. Enhanced Protected Mode adds new restrictions such as ensuring malicious code can't saturate the address-space in memory. It also introduces a "broker process" that shields access to personal information by granting temporary access to files from the browser only when enabled by the user.

Protecting the Endpoints

While PC and mobile clients are the most frequent targets of attacks, most experts agree Microsoft has effectively reduced many of the threats that plagued its server products—including Windows Server, Exchange, SQL Server and IIS—by applying the SDL model, which resulted in cleaner code and fewer vulnerabilities. Most see Windows Server as a much more secure platform thanks to the evolution of the user-authentication model in Active Directory and add-on offerings such as Active Directory Federation Services (ADFS) and Forefront Identity Manager. For example, Active Directory in Windows Server 2008 permitted IT pros to implement fine-grained password polices and added auditing capabilities. ADFS, a free add-on to Active Directory, provided the basis for single sign-on to enterprise systems.

Windows Server 8, now in beta, will offer improved security on a number of fronts. Dynamic Access Control (DAC) will provide a centralized way to provide policy management and governance to files. DAC allows IT pros to manually or automatically classify files, control access, add Rights Management Services encryption for sensitive Office documents and conduct audits.

"It's a completely different way of doing authorization for Windows files, and it provides a way to actually use external authorization," says Gartner Inc. analyst Mark Diodati.

Microsoft is also upgrading Active Directory Domain Services in Windows Server 8 by offering simplified access to both the datacenter, virtual machine and cloud services, allowing a single set of credentials.

"Right now, I'm skeptical because Microsoft has purely been an on-premises vendor," says Forrester Research Inc. analyst Andras Cser. "Obviously, their vested interest still lies with keeping things on-premises because that's where most of their revenue comes from. But this is a step in the right direction."

As Microsoft looks to tie Windows Server 8 and Active Directory to its cloud services, the company is also looking to avoid any miscues. It goes without saying that security

breaches with its flagship Office 365 and Windows Azure cloud platforms could be devastating—and could scare customers away from using cloud services.

In a sign of the times, in March Microsoft released a technology preview of its Microsoft Endpoint Protection for Windows Azure. The plug-in, an extension of the SDK, allows IT pros and developers to embed anti-malware into their Windows Azure instances. The company says the tool allows IT pros to import the anti-malware module into their roles definitions.

By deploying the anti-malware app into a Windows Azure service, users can have real-time protection, scanning, malware remediation, signature updates and active production. The latter feature issues reports about discovered threats to Microsoft.

The Pinnacle of Security?

It's hard to dispute that Microsoft has come a long way over the past 10 years in improving the security of its products, even if no one—including Microsoft—is saying "mission accomplished." With new threats evolving every day, coupled with advances in computing and new uses of technology, the next 10 years could be more challenging for Microsoft than the decade that just passed. Its key challenge will be getting its partners and customers to become more vigilant.

"I don't see any sign of Microsoft coming close to delivering the silver bullet that will solve the security problems the world is struggling with," says Paul Kocher, president and chief scientist of security consulting firm Cryptography Research. "They started out with the vision that they would make computers trustworthy, which was replaced by the realization that these are really hard problems and more difficult than people anticipated 10 years ago." R

Jeffrey Schwartz is executive editor of features for Redmond.

10 Common Security Blunders and How to Avoid Them

While IT managers are trained early on to avoid obvious threats, many still fail to watch out for the basics.

By Brien M. Posey

No matter how hard we fight, cyber threats are ever on the rise. Microsoft and the federal government are stepping up their war on organizations driving botnets. This is part of the problem. One of the biggest threats comes from within and failure to prepare for those battles is asking for trouble.

Even if you think your shop is doing all it can to avoid common security threats, you'd probably be surprised at how easily an outsider can find common—even silly—mistakes.

IT pros are overworked. It's only natural that even a top dog makes the occasional blunder. Over the years I've found many oversights in otherwise tightly secure organizations.

Here are some of the more common security mistakes I've run into.

1. Using Default Passwords

IT pros have long been told to use secure passwords and change them regularly. This idea seems to go out the window when it comes to network appliances. I've lost count of the number of times I've run into network appliances in production environments using default passwords.

Default passwords are a huge risk simply because they allow appliances to be easily compromised. This is especially true for network access points, but also applies to firewall appliances, intrusion-detection appliances and just about any other type of hardware appliance.

2. Setting up Weak Passwords

A few years ago, a neighbor asked me to set up his wireless

IMAGES FROM SHUTTERSTOCK

network. When it came time to enter the passphrase, I left the room and let him enter the phrase in private. Although I told my friend to use a strong passphrase, I had a hunch he'd use the name of his favorite sports team.

Later that night I connected to his wireless network from my house and after two or three tries was able to guess his passphrase. Once connected, I attached to his network printer and printed a message that his network was insecure and to call me when he was ready to fix it.

The point is that wireless passphrases are vulnerable to the same types of attacks as insecure passwords. Therefore, you should make a point of using strong wireless passphrases or at the very least avoiding those that others can guess.

3. Central Administrator Accounts

I used to work in a place where the entire administrative staff shared a single generic Administrator account. We had a disgruntled employee on the staff and she was constantly doing things to sabotage the network. Our audit logs showed her various actions as being performed by Administrator. Needless to say, a generic audit log entry wasn't enough for disciplinary action.

The IT manager was reluctant to create individual Administrator accounts, fearing multiple administrative accounts would increase the chances of a security breach. This meant the disgruntled administrator was able to continue with her shenanigans for quite some time.

Ever since, I've recommended to clients that they create two separate accounts for each member of the administrative staff. Both of these accounts should be personally identifiable. One account should lack administrative privileges and be used for all day-to-day activities. The other account should contain administrative privileges, but should only be used for administrative actions. Using this technique lowers the risk of a security breach, while ensuring that any administrative actions can be tracked back to the administrator who performed the action.

4. Failing to Utilize Group Policy Security

I recently read an article in which the author cautioned administrators to use Group Policy settings sparingly. It made the case that the more Group Policy settings are enabled, the longer the login process takes.

While I'm all for expediting the login process, I recommend taking full advantage of Group Policy security settings. Group Policy settings are the primary mechanism for ensuring the computers on your network adhere to your corporate security policy. Furthermore, if you need to make a change to your security, it's a lot more practical to modify a Group Policy setting than it is to try to update each computer individually.

5. Not Making Use of Local Security Policies

Although Group Policies are important, it's also important to make use of local security policies. Local security policies are often overlooked because they exist at the lowest level of the Group Policy hierarchy. It's usually considered a better practice to implement policy settings at a higher level, such as at the domain or Organizational Unit (OU) level of the Group Policy hierarchy. Even so, using local security policies is important.

This is the case because higher-level Group Policy settings only apply once a user logs in to a domain. If someone happens to log in to a workstation using a local account, then none of the higher-level Group Policy settings will be applied. The workstation's only defense at that point is the local security policies.

I'll be the first to admit that if someone logs into a workstation with a local account, then they can disable the individual elements within the local security policy. However, that only becomes a concern if the person who's logging in has malicious intent. There are plenty of perfectly legitimate reasons why someone might need to log into a workstation using a local account (such as to perform a repair or system maintenance). In these types of situations, the local security policy helps provide basic security.

6. Forgetting About Certificate Expirations

I have to confess this is one bonehead move I'm personally guilty of. Recently I took a couple weeks off and went to South America to do some extreme caving and scuba diving. While I was gone I left my smartphone turned off. When I got back to the United States, I turned my phone on, but couldn't get any e-mail.

I assumed my server must have crashed, or that my power or Internet connection was out. Living in the sticks, I lose Internet and electricity all the time, so I didn't panic.

When I finally got to my house 12 hours later, I found everything on my network functioning perfectly. While going through the troubleshooting process, I found the digital certificate for my Exchange Server had expired. The certificate was valid for five years, and just happened to expire while I was on vacation. Now I'm in the habit of documenting certificate expiration dates and setting up automated reminders to renew certificates before they expire.

7. Excessive Auditing

I took my first Windows certification class back in the '90s, and will never forget the lesson on event auditing. I was utterly amazed by the granularity with which events could be audited. At the same time, I was bewildered as to why enabling auditing was a manual process. I asked why Microsoft didn't enable all the auditing mechanisms by default. The instructor's response holds just as true today as it did back then.

Auditing every possible event is a bad idea for a couple of reasons. First, excessive auditing can degrade a server's

performance. CPU and disk resources are consumed by the auditing process, but when auditing is performed in moderation the resource consumption is no big deal. However, when you audit an excessive number of events, the auditing process can have a noticeable impact on the server's performance.

A more important reason for auditing in moderation is that, when you audit an excessive number of events, the event logs can quickly become huge. When this happens, it's nearly impossible to pinpoint the events you're truly interested in. Important security alerts blend in with all of the meaningless events that have been logged. That being the case, you should only log the events that are most relevant and would provide the most useful forensic information if an attack should occur.

8. Writing Down Passwords

When I first started working in IT, I lost count of the people who told me you should never, ever write down a password. In many ways this rule makes sense. After all, if you write down passwords there's a chance those passwords could find their way into the wrong hands. But I think the idea of never writing down passwords is incredibly shortsighted.

I agree user account passwords that are used on a day-to-day basis should not be written down. After all, these types of passwords expire on a regular basis and are easy enough to reset. However, there are other passwords that tend to be a bit more permanent and are used much less frequently.

One example is my wireless router password. I probably haven't logged into my router's Web interface in at least a year. I'm not even positive I remember the password correctly. That's why I have the router's password written down and locked in a safe with the rest of my network documentation. That way, if a problem ever does occur, I don't have to worry about trying to remember an obscure password that I haven't used in a while.

I recommend writing down semi-permanent and rarely used passwords. Of course, this is assuming you have a way to adequately protect the paper containing the passwords.

9. Ineffective Service Account Maintenance

In a Windows Server environment, system services are associated with a security account. Services can't start unless the service account is successfully authenticated. Most services make use of the Local System Account, but some services (such as the ones used by SharePoint 2010) require actual user accounts. In these types of situations, there are two mistakes that are commonly made.

One common mistake is creating an all-purpose service account. This is a mistake because service accounts are almost always assigned special permissions. These permissions allow the corresponding service to perform its intended tasks. When a single account is assigned to multiple services, the service account might begin to accumulate permissions that are far beyond those required to perform any one, single task. These excess permissions could allow an attacker to exploit a service to gain control of the system.

Wireless passphrases are vulnerable to the same types of attacks as insecure passwords.

The other common blunder related to service accounts is that administrators often require service account passwords to be changed on a regular basis. There's nothing wrong with resetting service account passwords, but you won't typically receive a reminder that the account is about to expire, and you'll have to update the service itself to use the new password. This usually means shutting down the service for a moment.

Service accounts can be a favorite target for hackers because they tend to use static passwords and might have permissions that exceed those of even an administrator (service accounts are typically able to act as a part of the OS, while admins are not). As such, it's a good idea to dedicate each service account to one specific service and give your service accounts names that disguise their true purposes. I recommend giving your service accounts names that blend in with your user accounts. For example, you might name a service account JSmith.

10. Failing to Have an Incident Response Plan

By far the most serious—and yet one of the most common—security blunders is not having an incident response plan. Imagine you walked into the office tomorrow and found you've been hacked. What do you do?

If you had to stop and think about it, you just demonstrated my point. It's important to develop a formalized incident response plan before a security breach occurs, so you and your staff will know exactly what to do. Initial actions you might take include disconnecting network cables, reviewing audit logs, verifying the integrity of your data and rebuilding affected servers.

The appropriate response will vary from one organization to the next, and it's critically important to come up with a security incident response plan that fits your organization's needs. R

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.

Why Employee Monitoring Matters

Some companies demand that IT track Web use or go even deeper into user behavior. Here are some tips on how to do it right and what tools to use.

By Derek Schauland

Several years ago a friend asked what could happen if her company tracked Internet use. While this might sound a bit naïve today, back then monitoring wasn't so commonplace.

Depending on your industry and the norms that apply (or your company's particular values and policies), your monitoring might be worlds different from the level at the company just up the street. Regardless of the level of intrusion, all content or usage tracking should be disclosed to users. Your company should have a clear policy, let employees know what it says, and monitor only in a way that matches that policy. Your shop might own the equipment and the Internet pipe and all of that, but employees still assume some level of privacy or least full disclosure of when and how they're being observed or tracked.

Internet usage monitoring isn't packet capture. Sure, the packets sent out through a firewall or other device when you browse the Internet to visit the Disney Store Web site are logged by the firewall, and the IP address or maybe even the URL is contained within the packet and can be seen by someone designated to sift through those logs. This is typically used to troubleshoot network issues or at the network level. General Internet usage monitoring is much simpler.

With general Internet usage monitoring, an application is installed on the computers within an organization or on an appliance sitting between company computers and the Internet where all the Internet traffic passes through. When it passes through and onto the appliance, the details are logged and the traffic goes on its merry way.

IMAGES FROM SHUTTERSTOCK

Monitor Usage and Block Content

There are devices and software packages available that can not only monitor traffic, but also allow for certain Web sites or categories of sites to be blocked (see "Internet Usage Monitoring Solutions"). This does a few things. First, it prevents content that an organization deems inappropriate from being viewed on company resources. Second, some of these products perform tasks that users actually appreciate, such as blocking advertisements on Web pages—especially those ads that are considered unacceptable. Because many of these ads are sourced at domains such as doubleclick.net, they can be singled out, which definitely improves the Internet experience.

There are different levels of monitoring, and these should be considered before jumping into a solution. General monitoring for Internet use only is pretty normal today, where surfing is logged. Other products are much more user-level or granular in what they log. Trapping passwords and keystrokes on your corporate network takes monitoring a tad too far, one could argue, but those products exist as well.

As mentioned, it makes sense to have an acceptable use policy, let all employees know, then advise them you're running a Web monitoring program. If you're planning to block traffic you should certainly tell them that as well. If they know Internet use is being looked at, they'll naturally cut down

Internet Usage Monitoring Solutions

GFI WebMonitor Priced per seat, this software can be used as a standalone monitoring tool or in conjunction with other security products such as Microsoft Forefront Threat Management Gateway. It provides statistics about where your users are headed on the Internet and how much time they spend on specific sites. The new 2012 version also monitors search keywords.
gfi.com

Websense This solution is one I consider the granddaddy of them all. It monitors Web traffic, e-mail and other items including mobile devices. Some organizations also use this product to manage and monitor content within their e-mail systems to prevent non-work-related content through that channel as well.
websense.com

Barracuda Web Filter This product is sold as an appliance that plugs in to your network, sitting between your users and the Internet. Web traffic is given one path to the Internet, passing directly through the Barracuda box. Featuring reporting and easy-to-access information down to the user level, the device is easy to get up and running. I did find that, when using this device, some noise was found for things that continually refresh, such as weather sites or other perfectly acceptable destinations. Once you've started looking at the traffic, it's pretty interesting to see which sites are most used. In addition to being available as a standalone appliance, this product is also available in virtual appliance form.
barracudanetworks.com

Spector CNE Investigator This product not only records where an employee might be headed on the Web, but also any programs used, keystrokes typed and other actions taken on the PC where it's installed. When the application is installed, it can be run in stealth mode to prevent detection or access to the software on the local system. As actions are recorded, the information is sent securely to a central location where only administrators can access it. Sessions captured can be played back to follow the actions of a user during a specific time period.
spectorcne.com

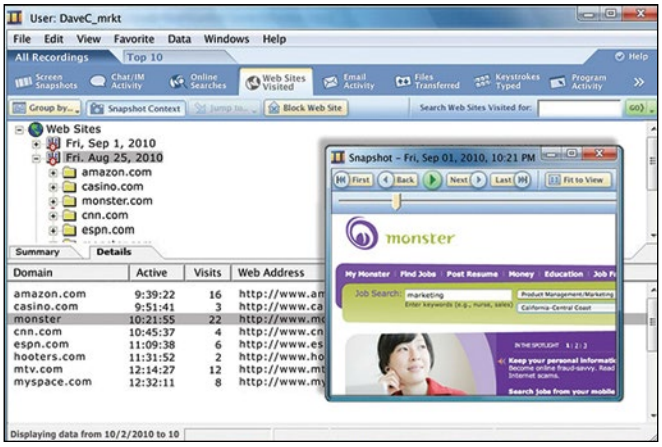
EfficientLab Work Examiner Monitors activity and provides reporting to determine where productivity could be improved and help the organization ensure resources aren't being misused while an employee is working. In addition to Web monitoring and access tracking, this application also provides tools for time tracking.
workexaminer.com

CurrentWare BrowseReporter Allows monitoring of Web access and use by employees. By capturing all URLs visited along with on-demand screen capture, BrowseReporter is designed to provide a holistic view into what's going in and out of an organization via the Internet. An interesting feature of this application is idle timeouts, which allow a browser to be deemed idle after a configured period of inactivity. If the session is idle, it can be excluded from reports to reduce the noise recorded by the application.
currentware.com

NesterSoft WorkTime Like other products listed, WorkTime records all PC activity and can be useful outside of the Web monitoring space. When it comes to monitoring the Internet, NesterSoft captures useful information about browser sessions including sites visited, URLs, start time and page titles.
nestersoft.com

Wavecrest CyBlock This monitoring product comes in many forms, including an appliance (much like the Barracuda), a plug-in to Microsoft Internet Security and Acceleration and Forefront Threat Management Gateway server products, or standalone proxy server software. It can prevent access to categories of Web sites or applications and provide real-time statistics and analysis to show administrators what employees are using on the Internet and when.
wavecrest.net

—D.S.



Keystroke and Web traffic recording with Spector CNE Investigator.

on non-work-related Internet usage. You'll also likely cut down on help desk calls over certain pages coming up with administrator blocked notifications or errors.

My company monitors Internet usage and blocks some traffic, which seems to work pretty well. It's definitely nice to have fewer online ads. However, the fact that most appliances create filters by group or category is interesting. Alcohol, tobacco and firearms categories are usually lumped together, which in most cases is great. But I work for a company that produces ingredients for beer. Almost immediately after deploying a Web monitoring appliance, we had to create rules to make sure we weren't cut off from our customers' Web sites. That problem has mostly been addressed, but it was certainly no fun undoing a good chunk of a blacklist. The biggest lesson is to know what filter/monitor drives are on for filtering. This way you can make adjustments quickly with as little impact to the user as possible.

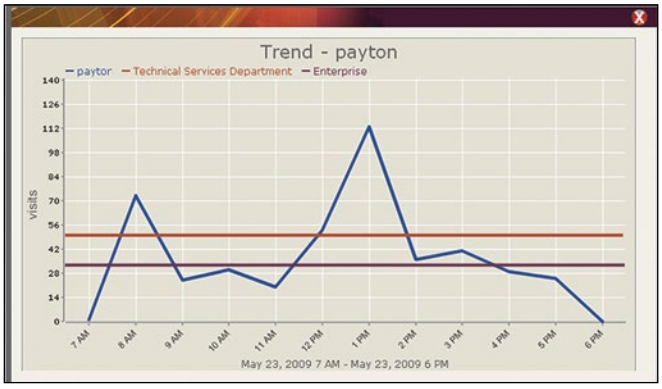
Helpful for Both Sides

I've heard of companies wanting to protect the "privacy" of their employees and feeling they could trust their employees to do the work they were paid to do. This is probably true for most companies; I believe people are generally good spirited. But there are times when things get out of control and something needs to be done to protect the company.

Suppose someone was constantly surfing the Internet and disrupting those around him, either by talking incessantly about things he saw or leaving stuff playing on the computer screen and shuffling off to another area. If an organization wanted to take action against this behavior, it might not have a leg to stand on without monitoring.

Monitoring can help employees, too. Imagine an employee working the late shift. There aren't many people around and it's a slow night, so he decides to surf the 'Net and gets hit with malware. Malware is bad enough, but this one comes in the form of pop-ups exposing all kinds of filth. A manager seeing this later, with a different user at the PC's helm, might think that user was the one irresponsibly surfing. Here monitoring might help pinpoint the user who was actually logged on rather than the one assumed to be the cause of the problem.

When someone thinks they're being watched their behavior changes, and in some cases this justifies the monitoring policy and tracking software in the first place.



Trending and protocol monitoring using Wavecrest CyBlock.

Making Exceptions

Because many Web monitoring tools block sites that might seem (but not actually be) inappropriate, there are cases when users have legitimate needs for sites the software declares off-limits. Fortunately, just like many anti-spam applications, Web monitoring tools have whitelisting capabilities. This lets certain sites within a category stay accessible while the rest of the category is blocked. Let's say your organization sells a product to a few companies within a category, but other sites in the same category are not appropriate for browsing. The customer sites can be whitelisted, but the remaining items in the category will be blocked.

Keep in mind that most of these products will both filter and block traffic. R

Derek Schauland has worked in technology for 15 years in everything from a help desk role to Windows systems administration. He has also worked as a freelance writer for the past 10 years. He can be reached at derek@derekschauland.com.

Web Monitoring Tips

- Inform employees you're tracking their Internet usage. It will deter them from going to inappropriate sites, improve productivity and let them know exactly where the company stands.
- Decide if you need to track sites visited or go a step further and block access to certain URLs.
- Some tools track keystrokes and capture passwords. Decide if you need those, but in many cases they're excessive.
- In addition to making users more productive and keeping them off inappropriate sites, Web monitoring is also useful for blocking sites that produce malware.