Published on *InfoWorld* (http://www.infoworld.com)

10 crazy IT security tricks that actually work

By Roger A. Grimes
Created *2012-07-09 03:00AM*

Network and endpoint security may not strike you as the first place to scratch an experimental itch. After all, protecting the company's systems and data should call into question any action that may introduce risk. But IT security threats constantly evolve, and sometimes you have to think outside the box to keep ahead of the more ingenious evildoers.

And sometimes you have to get a little crazy.

[Find out how to block the viruses, worms, and other malware that threaten your business, with hands-on advice from expert contributors in InfoWorld's "Malware Deep Dive" PDF guide. | Keep up with key security issues with InfoWorld's Security Adviser blog and Security Central newsletter.]

Charles Babbage, the father of the modern computer, once said, "Propose to a man any principle, or an instrument, however admirable, and you will observe the whole effort is directed to find a difficulty, a defect, or an impossibility in it. If you speak to him of a machine for peeling a potato, he will pronounce it impossible: If you peel a potato with it before his eyes, he will declare it useless, because it will not slice a pineapple."

The world of network security is no different. Offer a new means for IT defense, and expect to meet resistance. Yet, sometimes going against the wave of traditional thinking is the surest path to success.

In that vein, we offer 10 security ideas that have been -- and in many cases still are -- shunned as too offbeat to work but that function quite effectively in helping secure the company's IT assets. The companies employing these methods don't care about arguing or placating the naysayers. They see the results and know these methods work, and they work well.

Innovative security technique No. 1: Renaming admins
Renaming privileged accounts to something less obvious than "administrator" is often slammed as a wasteful, "security by obscurity" defense. However, this simple security strategy works. If the attacker hasn't already made it inside your network or host, there's little reason to believe they'll be able to readily discern the new names for your privileged accounts. If they don't know the names, they can't mount a successful password-guessing campaign against them.

Even bigger bonus? Never in the history of automated malware -- the campaigns usually mounted against workstations and servers -- has an attack attempted to use anything but built-in account names. By renaming your privileged accounts, you defeat hackers and malware in one step. Plus, it's easier to monitor and alert on log-on attempts to the original privileged account names when they're no longer in use.

Innovative security technique No. 2: Getting rid of admins
Another recommendation is to get rid of all wholesale privileged accounts: administrator, domain admin, enterprise admin, and every other account and group that has built-in, widespread, privileged permissions by default.

When this is suggested, most network administrators laugh and protest, the same response security experts got when they recommended local Administrator accounts be disabled on Windows computers. Then Microsoft followed this recommendation, disabling local Administrator accounts by default on every version of Windows starting with Vista/Server 2008 and later. Lo and behold, hundreds of millions of computers later, the world hasn't come crashing down.

True, Windows still allows you to create an alternate Administrator account, but today's most aggressive computer security defenders recommend getting rid of all built-in privileged accounts, at least full-time. Still, many network admins see this as going a step too far, an overly draconian measure that won't work. Well, at least one Fortune 100 company has eliminated all built-in privileged accounts, and it's working great. The company presents no evidence of having been compromised by an APT (advanced persistent threat). And nobody is complaining about the lack of privileged access, either on the user side or from IT. Why would they? They aren't getting hacked.

Innovative security technique No. 3: Honeypots
Modern computer honeypots have been around since the days of Clifford Stoll's "The Cuckoo's Egg," and they still aren't as respected or as widely adopted as they deserve to be. A honeypot is any computer asset that is set up solely to be attacked. Honeypots have no production value. They sit and wait, and they are monitored. When a hacker or malware touches them, they send an alert to an admin so that the touch can be investigated. They provide low noise and high value.

The shops that use honeypots get notified quickly of active attacks. In fact, nothing beats a honeypot for early warning -- except for a bunch of honeypots, called a honeynet. Still, colleagues and customers are typically incredulous when I bring up honeypots. My response is always the same: Spend a day spinning one up and tell me how you feel about honeypots a month later. Sometimes the best thing you can do is to try one.

Innovative security technique No. 4: Using nondefault ports
Another technique for minimizing security risk is to install services on nondefault ports. Like renaming privileged accounts, this security-by-obscurity tactic goes gangbusters. When zero-day, remote buffer overflow threats become weaponized by worms, computer viruses, and so on, they always -- and only -- go for the default ports. This is the case for SQL injection surfers, HTTP worms, SSH discoverers, and any other common remote advertising port.

Recently Symantec's pcAnywhere and Microsoft's Remote Desktop Protocol suffered remote exploits. When these exploits became weaponized, it was a race against the clock for defenders to apply patches or block the ports before the worms could arrive. If either service had been running on a nondefault port, the race wouldn't even begin. That's because in the history of automated malware, malware has only ever tried the default port.

Critics of this method of defense say it's easy for a hacker to find where the default port has been moved, and this is true. All it takes is a port scanner, like Nmap, or an application fingerprinter, like Nikto, to identify the app running on the nondefault port. In reality, most attacks are automated using malware, which as stated, only go for default ports, and most hackers don't bother to look for nondefault ports. They find too much low-hanging fruit on default ports to be bothered with the extra effort.

Years ago, as an experiment, I moved my RDP port from 3889 to 50471 and offered a reward to the first person to find the new port. Two people discovered the port right away, which was no surprise; because I told them what I did, it's easy to discover the right spot. What blew me away is that tens of thousands of hacker wannabes, scanning my system for the new port using Nmap, didn't realize that Nmap, if left to its own defaults, doesn't look on nondefault ports. It proved that by doing a simple port move you significantly reduce your risk.

Innovative security technique No. 5: Installing to custom directories
Another security-by-obscurity defense is to install applications to nondefault directories.

This one doesn't work as well as it used to, given that most attacks happen at the application file level today, but it still has value. Like the previous security-by-obscurity recommendations, installing applications to custom directories reduces risk -- automated malware almost never looks anywhere but the default directories. If malware is able to exploit your system or application, it will try to manipulate the system or application by looking for default directories. Install your OS or application to a nonstandard directory and you screw up its coding.

On many of my honeypots, I install the OS to nondefault folders -- say, in C:/Win7 instead of C:/Windows. I usually create the "fake" folders that mimic the real ones, had I installed the software and taken the defaults. When my computers get attacked, it's easy to find complete and isolated copies of the malware hanging out in the C:/Windows/System32 folder.

Changing default folders doesn't have as much bang for the buck as the other techniques mentioned here, but it fools a ton of malware, and that means reduced risk.

Innovative security technique No. 6: Tarpits
My first experience with a tarpit product was LaBrea Tarpit. It was developed during the outbreak of the Code Red IIS worm of 2001. Worms readily replicate to any system that matches their exploit capabilities. LaBrea worked by answering connection attempts for addresses not already assigned to legitimate machines. It would then answer and tell the worm to connect, then spend the rest of the time trying to slow down the worm, using various TCP protocol tricks: long timeouts, multiple retransmissions, and so on.

Today, many networks (and honeypots) have tarpit functionality, which answers for any nonvalid connection attempt. When I penetration-test these networks, my attacks and network sweep scanning attacks slow to a crawl -- they're unusable, which is exactly the purpose. The only downside: Tarpits can cause problems with legitimate services if the tarpits answer prematurely because the legitimate server responded slowly. Remember to fine-tune the tarpit to avoid these false positives and enjoy the benefits.

Innovative security technique No. 7: Network traffic flow analysis
With foreign hackers abounding, one of the best ways to discover massive data theft is through network traffic flow analysis. Free and commercial software is available to map your network flows and establish baselines for what should be going where. That way, if you see hundreds of gigabytes of data suddenly and unexpectedly heading offshore, you can investigate. Most of the APT attacks I've investigated would have been recognized months earlier if the victim had an idea of what data should have been going where and when.

Innovative security technique No. 8: Screensavers
Password-protected screensavers are a simple technique for minimizing security risk. If the computing device is idle for too long, a screensaver requiring a password kicks in. Long criticized by users who considered them nuisances to their legitimate work, they're now a staple on every computing device, from laptops to slates to mobile phones.

I remember one time leaving my smartphone in a cab, right after an argument with the cab driver over the bill (he had taken me on a much longer, more circuitous route than necessary). I immediately considered that phone long gone. I was worried because I had just chatted with my wife, so the phone was open and exposed. I store my passwords and other personal information on the phone, although slightly modified so that anyone reading it directly wouldn't know the true passwords or numbers. I was more worried about the contact information for my wife, daughters, and other loved ones. Luckily, I knew my screensaver would kick in momentarily. I never found the phone, but I didn't get any weird calls or charges either.

Innovative security technique No. 9: Disabling Internet browsing on servers
Most computer risk is incurred by users' actions on the Internet. Organizations that disable Internet browsing or all Internet access on servers that don't need the connections significantly reduce that server's risk to maliciousness. You don't want bored admins picking up their email and posting to social networking sites while they're waiting for a patch to download. Instead, block what isn't needed. For companies using Windows servers, consider disabling UAC (User Account Control) because the risk to the desktop that UAC minimizes isn't there. UAC can cause some security issues, so disabling it while maintaining strong security is a boon for many organizations.

Innovative security technique No. 10: Security-minded development
Any organization producing custom code should integrate security practices into its development process -- ensuring that code security will be reviewed and built in from day one in any coding project. Doing so absolutely will reduce the risk of exploitation in your environment.

This practice, sometimes known as SDL (Security Development Lifecycle), differs from educator to educator, but often includes the following tenets: use of secure programming languages; avoidance of knowingly insecure programming functions; code review; penetration testing; and a laundry list of other best practices aimed at reducing the likelihood of producing security bug-ridden code.

Microsoft, for one, has been able to significantly reduce the number of security bugs in every shipping product since instituting SDL. It offers lessons learned, free tools, and guidance at its SDL website.

This story, "10 crazy IT security tricks that actually work," was originally published at InfoWorld.com. Follow the latest developments in security at InfoWorld.com. For the latest developments in business technology news, follow InfoWorld.com on Twitter.

Security Anti-virus Application Security Data Security Network Security Password Security