CSO
SECURITY AND RISK

From: www.csoonline.com

The Seven Deadly Sins of Network Security

Companies that suffer serious network security breaches have almost always committed one (or all) of 7 deadly sins. Is your company guilty?

by Bill Brenner, Senior Editor, CSO

December 10, 2008

Anyone worth their salt in information security will tell you a solid defense is built upon multiple layers of technology, policy and practice. That's defense-in-depth.

The technology layers are a critical piece of that puzzle -- of course. But companies that suffer a major network breach have frequently failed on a more fundamental level. Here are the deadly **network security sins** experts say are rampant in the corporate world. Avoid these sins and you will have taken a critical step toward a secure network.

Not measuring network security risk

This sin typically involves a failure to take a thorough measurement of the company's most important assets and network configurations surrounding those assets. As the saying goes, you can't protect the crown jewels without first knowing what they are and where they are.

Chuck McGann, manager of corporate information security services for the U.S. Postal Service, is among those who cited the "failure to have a network topology diagram or discovery software to identify what is on your network and what it is doing."

When a company fails to take an accurate measurement of risk, the powers that be are often lulled into the false sense of comfort that comes with simply having antivirus software and a firewall, says Michael Leigh, senior information security manager at Cisco Systems. The bad news here is that some of that technology can become the very problem the organization sought to prevent.

"I find that a number of organizations believe their security appliance/devices (routers, firewalls, switches, etc) are secure and do not layer their defenses around these devices," Leigh says. "Too often these devices are the toe hold into an organization."

Ken Smith, a security solutions architect at Forsythe Technology, says implementing security controls and policies without first understanding business needs and requirements is a problem he has witnessed many times. "It's the primary reason that security practitioners are often thought of as rigid or not adding value to the organization," he says. "When this is the case, users will come up with workarounds that could be worse than the problem you are trying to prevent in the first place."

Thinking compliance equals security

Typically the sin committed by upper management, this is the case where a company has invested a lot of time and treasure on meeting the requirements of government regulations and industry standards like HIPAA or PCI DSS, then dropping the ball once all the boxes on a compliance checklist have been checked off.

Experts unanimously say that, while these regulations can provide a good start on network security, by no means do they include all the requirements necessary to protect data.

The compliance-equals-security view is similar to the flaw of looking at security as a project rather than a process, says Timothy Brush, an independent security consultant based in Canada. Upper management looks at security as a project that must be dealt with, typically because of compliance concerns, then loses interest.

"The security landscape -- technologies, vendors, attack vectors, vulnerabilities, etc. -- is constantly changing," Brush notes. "The latest technology -- firewall, IDS/IPS, identity management systems, vendor-driven technology du jour -- or procedure -- policy, standard, framework, business process -- may increase an organization's security posture for the moment," but probably not a year or five down the road.

Daniel Blander, a CISM, CISSP and president of Techtonica Inc. in Los Angeles, has seen this sin committed over and over again, and mentioned it in a recent report on post-PCI audit troubles.

"Having worked on two PCI projects, the biggest challenge is typically management's view, 'Well, were compliant, so we're done.'" he says. "Some parts of management understand the 'why' of PCI, but don't understand overall risk management. Maintaining attention after the fact is the biggest challenge."

Overlooking the people

A similar thread in all the sins mentioned is a tendency of organizations to look at security as a mostly technological issue, ignoring that the biggest dangers emanate from the people using the machines without really understanding what they're doing -- or that unwary employees can be exploited through common social engineering tricks.

"Too many focus on tools for the infrastructure within their organization and budget," says Matt Polatsek, a senior security engineer at Hughes Network Systems in the Washington D.C. area. "The people and/or employees are so often overlooked in either purposeful sabotage or inadvertent disclosure."

Firewalls, VPNs, IDS/IPS, SIEM tools, remote access, encryption, switches, and routers are all great and fun to play with, he says. But in the end, too few see the value in security awareness among the larger workforce and often lack a viable, enforceable policy on what users can and can't do on company machines, he adds.

Gary Bahadur, a Miami-based operations and security technology executive and a former VP at Bank of America, cited the problem at the top of his personal list.

"Not educating/training the end user in basic security measures is a problem," he says. "All the security and money spent is useless if the end user continues to click on e-mail links, tape the password to the computer and surf porn sights. The biggest bang for the security buck is user education."

Too much access for too many

Most respondents agreed a lack of access control is the sin that has sent many a company down the road to trouble.

"The biggest failure I've seen is the lack of management support for the necessary expenditures and for the ongoing need to have a clear, working policy on who has authority to do what, who's responsible for granting or denying access, who's responsible for vetting changes, and having it all done in such a manner as to not be too cumbersome on the operations of the company," says Toivo Voll, a network administrator for an educational institution in the southeast.

George Johnson, chief security officer at the National Center for Crisis and Continuity Coordination (NC4), says IT shops often assign everyone administrative access to reduce the workload tighter controls involve. This, he says, is a recipe for a massive compromise.

But the opposite practice of allowing only executives administrative access while locking everyone else out is fraught with danger as well.

"Hackers are targeting execs -- a tactic called 'whaling' -- so this is a huge risk," Johnson says. "It also severely damages the credibility of the security mission when it is obvious that the boss doesn't care about it. Culture springs from the top."

This summer's incident in San Francisco provides another illustration of the risks of putting too much control in one person's hands. A network administrator for the city was able to lock everyone else out of a critical system.

Lax patching procedures

A common security failure often stems from a company's inability to keep up with all the patches needed on the network's various devices. Proof of this problem was offered in a recent study from Verizon showing that 90 percent of successful exploits these days involve vulnerabilities for which a patch has been available for six months or longer.

"For the overwhelming majority of attacks exploiting known vulnerabilities, the patch had been available for months prior to the breach," Verizon says on page 15 of its 2008 Data Breach Investigations Report. "Also worthy of mention is that no breaches were caused by exploits of vulnerabilities patched within a month or less of the attack."

The bad guys know a lot of companies are slow to patch, and so they continue to cook up exploits for the older vulnerabilities, experts say. In fact, security experts say, worms like Blaster and Sasser -- launched four to five years ago against vulnerabilities for which patches were made available around the same period -- are still in wide circulation today.

Dan Ward, an IT security analyst at Acxiom, cites this as one of the major sins on his personal list. This problem, he says, extends not just to poor operating system patching, but also middleware, application and even device driver security updates.

(See Ed Ziots's recent column for advice on How to Handle Security Patches with Sanity.)

6. Lax logging, monitoring

The final item on the list involves the failure of many organizations to keep an eye on all the activity logs coming out of the various devices on the network. As McGann points out, a company must know what's going on in the network in order to secure it.

Ward agrees. "Log management is one of those issues that no one really likes to deal with," he says. "But since we're security professionals, we really need to dig into our log data and understand what's happening at all levels of the end-user chain."

7. Spurning the K.I.S.S. principle

It has been said that in the art of network security one must observe the K.I.S.S. principle -- "keep it simple, stupid," or "keep it simple for security." Unfortunately, networks are getting increasingly complex as companies bolt one device onto the next, often configuring things badly along the way.

Add the failure to segment certain parts of the network from other parts and you have a recipe for disaster.

"What can I say? Complexity is bad, very bad," Brush says.

Nick Puetz, director of data security at FishNet Security, says trusted networking is one of the founding concepts of IT security. However, while most companies will spend millions of dollars to secure their perimeter, "they don't take any time to segment their internal network."

As a result, it becomes impossible to get a grip on where sensitive data is flowing from one part of the network to the next. If you can't be certain where all the data is on the network, protecting it is exceedingly difficult. It's also the type of thing compliance auditors frown upon.

http://www.csoonline.com/article/470095/the-seven-deadly-sins-of-network-security
http://www.csoonline.com/article/print/470095