

SCM: The “Blocking and Tackling” of IT Security

When it comes to today’s threats, it’s back to basics. Security configuration management means getting serious about fundamentals, like hardening ever-changing IT configurations and keeping them that way.

Cloud computing. Virtualization. Social networking. IT consumerization. What do these trends all have in common? Besides promising to radically change the face of corporate technology today, they create threat vectors that can leave companies vulnerable to a whole new world of attacks, expanding the potential for data breaches. Despite these rising threats, uncertain economic times are resulting in shrinking IT budgets.

Fewer dollars and less IT staff devoted to securing infrastructures have security professionals struggling to keep up. The IT security market is overflowing with options designed to protect corporate infrastructure from unauthorized access; some essential, some not, but all marketed as critical. As vendors work up a fever pitch over the latest threats and the products that protect against them, it’s easy for security professionals to forget the basics. Yet, as with any discipline, the basics must be addressed in order for strategies to succeed.

Getting back to basics means repeatedly taking a hard look at one’s security environment, crossing all the T’s and dotting all the I’s. And then doing it again. After all, if a basic level of security isn’t maintained and a breach occurs, the blame falls squarely on the shoulders of the security professional. Still, in the realm of security basics, hardening security configurations across corporate IT assets may seem like reverting back to Security 101. But when attackers troll for the least-defended environments, such security measures are exactly what it takes to force attackers on to greener pastures. Think about it — it’s why a burglar looks for an open window or door before he breaks one.



Attackers in the House

Data breaches continue to rank as a top threat to corporate environments, as more and more attackers successfully find their way into networks.

According to Verizon’s 2011 Data Breach Investigation Report, data loss through cyber attacks decreased significantly in 2010, but the total number of breaches was higher than ever. The number of compromised records involved in data breaches dropped to 4 million in 2010, down from 144 million in 2009. Yet there were approximately 760 breaches last year, the largest number since the report’s inception.

This means that while attackers don’t always steal data, their ability to gain unauthorized access continues to grow. Considering that many attacks today aren’t isolated incidents — attackers often work to break down a network’s security over time — breaches that don’t result in immediate data theft may still be dangerous as they lay the groundwork for future harm. In 2010 outsiders were responsible for more data breaches than in the past, totaling 92 percent, which Verizon attributes to the significant increase in smaller external attacks.

“Right now, the threat of breaches from external parties is the No. 1 issue my clients worry about,” says Daniel

Blander, CEO & Co-Owner of InfoSecurityLab, which builds worldwide information security and risk management programs for businesses.

And while the theft of customer or employee personal data and corporate financial data is still concerning, companies today are most worried that their intellectual property (IP) could be stolen as a result of unauthorized network access. “IP is getting higher and higher on executives’ lists of worries. Companies really care about competitors finding out their project ideas and having them show up somewhere else in the world with some other company’s name on it,” says Blander.

In fact, in its June report entitled “Perceptions About Network Security,” the Ponemon Institute found that 80 percent of the 583 IT security practitioners in the U.S. who responded to a survey said they had experienced at least one data breach. Of those who were able to calculate the cost of security breach — including cash outlays, internal labor, overhead, revenue losses, and other related expenses — 41 percent said the breach cost them \$500,000 or more.

What’s more, 53 percent of respondents to the Ponemon survey said they have little confidence that they would be able

to avoid one or more cyber attacks in the next 12 months. If these companies haven’t focused on laying a sturdy foundation for their company’s security, they have good reason to worry.

An Ounce of Prevention

Perhaps most disturbing, however, is the simple fact that the vast majority of breaches that occur could have been prevented. Verizon’s report says that 92 percent of last year’s attacks were not considered ‘highly difficult,’ and 96 percent could have been avoided through simple or intermediate control. What’s more, 50 percent of the breaches involved hacking and 49 percent involved malware (with some overlap that involved both) and both of these vectors prey primarily on weakly configured or loosely monitored systems.

While there’s no such thing as an IT environment that is 100 percent secure, taking fundamental steps to assess and harden IT systems is the basic “blocking and tackling” of IT security that removes the root cause of the vast majority of breaches. These steps include:

- ✓ Assess and inventory configurations on all servers and devices, and compare the results to some understood, recognized security standard (like CIS, NIST, or ISO-27001)
- ✓ Gain immediate, real-time insight into any changes to the files, configurations items and states that define this security standard

“Blocking and tackling” for security professionals means going back to basics and eliminating the “easy in’s” preyed on by attackers in the Verizon report, like open ports and unused services, the use of default or easily guessed administrator passwords, or improperly configured firewalls. “Blocking and tackling” for IT security teams also means keeping continuous watch on these systems, to detect the clues that indicate attacks in prog-

ress, like security controls disabled by anti-forensic activities, oddly elevated permissions, or unexpected changes to critical files.

Security configuration management solutions are built to make these issues visible to IT security professionals, and to give them the information and tools they need to manage them in the most automated way possible.

Hardening Systems is Job #1

Yet in complex corporate IT settings, it's easy to understand how these basic steps to security are overlooked. Software deployments, upgrades and patches are constantly changing the computing environment, and so maintaining standard configurations becomes difficult. Even the smallest changes can affect how permissions are set or which ports are to be used. Security professionals need help; they need an end-to-end view of the entire IT infrastructure so they can be kept informed of configurations, detect changes to standard configurations, and correct as needed.

Security Configuration Management (SCM) tools play an essential role in securing today's networks by providing security professionals with that ongoing, base level of assurance from which they can build their security strategies.

"Most attacks are targets of opportunity; the attacker is bouncing around until he finds a weakly defended system, and then uses that to wriggle into a network of connected machines. Because of that reality, hardening systems is Job #1," says Michael Thelander, director of product marketing with Tripwire. "If it's too hard for the passing hacker, worm, or malware, the attacker may just pass on to less defended targets."

SCM helps security experts cover the basics:



80% of the IT security practitioners in the U.S. who responded to a survey said they had experienced at least one data breach.

41% of those who were able to calculate the cost of security breach said the breach cost them \$500,000 or more. Including cash outlays, internal labor, overhead, revenue losses, and other related expenses.

SOURCE: Ponemon Institute report *Perceptions About Network Security*
BASE: 583 IT security practitioners

- ✓ It provides a base level of assurance by defining hardening and security guidelines that establish a company's basic known and trusted state, building the foundation of security;
- ✓ It takes an end-to-end approach and offers the best value for a company's security dollars because it can exist in every piece of the infrastructure. Security professionals can harden their servers, desktops, firewalls, switches, virtual systems, applications, databases, and more with one solution;
- ✓ Done correctly, it provides integrated monitoring capabilities that detect and act when configurations change unexpectedly
- ✓ It leverages third-party security benchmarks, and therefore doesn't require the lengthy, involved creation of custom rules in order to be effective
- ✓ It's an automated solution that can in many cases re-test configuration states when a change is detected
- ✓ When used in conjunction with Security Information and Event Management (SIEM) tools, it helps narrow the field so security professionals can more quickly pinpoint the problem.

By leveraging SCM, companies can increase the overall level of difficulty that attackers are met with upon attempting to gain access, while also reducing the attack surface. These tools also allow companies to measure their level of security and reduce the amount of work required by other security tools, such as SIEM products.

With SCM "you're creating a baseline of security and you have the opportunity in doing that to eliminate a very large percentage of weaknesses," says InfoSecurityLabs' Blander. Commercial software is always shipped with vulnerabilities, and that's something companies must deal with. "We must build our systems with a level of security to eliminate weakness, to a level that is better than the settings software manufacturers provide, to raise the expected level of security. If we don't pay attention to those, we allow for weaknesses."

A Realistic View of Security

Beyond technology, many IT professionals must work to change the corporate mindset regarding security. Companies today prefer to believe that a data breach won't happen to them

— they think they’re too small, too far off the radar, or don’t deal in enough sensitive information to be a fruitful target. The security professional’s job is to re-educate the organization for its own good. High profile, brand-name cases like the Sony breach garner most of the news attention, but the Verizon report showed a 230 percent increase in attacks against small companies of 100 or fewer employees. Clearly, there’s no such thing as “too small” or “too mundane.”

Given the high likelihood that a data breach will occur, security professionals must shift the conversation from “What will happen if we suffer a breach” to “We are highly likely to suffer a breach, let’s talk about strategies for rapid detection and minimal loss.” It isn’t easy for security professionals to draw attention to their companies’ security weaknesses, but being able to face the reality of a potential breach means they can be more proactive about dealing with the consequences.

“The likelihood of a breach is so high, it’s incumbent on them to explain to others that this is the state of the world,” says Tripwire’s Thelander.

This is another area where SCM can help, by closing the gap between the time of breach and detection, thus ensuring that when a breach does happen it will be detected as soon as possible to minimize impact. Implementing this technology raises the confidence of a company’s executives regarding overall security, and also sends a message to customers that a company is taking the necessary steps to protect their data.



“From a sales and marketing perspective, SCM lets us demonstrate to the customer that if they go with us, we’re thinking about their data and protecting their data — it helps us put a little wedge between us and the competition.”

— Art Taylor, president and CEO, Benefit Allocation Systems

“From a sales and marketing perspective, SCM lets us demonstrate to the customer that if they go with us, we’re thinking about their data and protecting their data — it helps us put a little wedge between us and the competition,” says Art Taylor, president and CEO of Benefit Allocation Systems, which provides a web-based employee benefits administration service. “For me, SCM lets me put my head on the pillow each night; it gives me a level of insurance.”

Taylor went to back to security basics, and he can sleep at night.

Building the Right SCM Toolkit

When getting back to those security basics, an effective SCM toolkit is about as fundamental as it gets. But remember all tools are not created equal. So security professionals should fill their toolkits with solutions that are purpose-built to provide end-to-end protection and facilitate the mandates to prevent, detect, and correct.

✓ **PREVENT:** SCM tools must be able to assess IT configurations against a wide range of policy and platform

configurations to prevent vulnerabilities from the onset;

✓ **DETECT:** The right tools should be able to detect changes to configuration states and files in real time, including changes that occur at the server, database, directory server, and network device level. They should also feed real-time information to policy management tools to provide truly continuous monitoring of files and configurations;

✓ **CORRECT:** SCM tools should also provide an automated way to repair broken or misaligned security configurations using role-based workflows, detailed reporting, and fully executable scripts that speed remediation time, reduce risk, and save time and money.

When all three of these SCM capabilities are rolled into one complete solution, getting back to those security basics gets a little easier. That’s certainly a best practice to strive for — especially when the devastating march of security breaches goes on and on and on. ■