

A Race Against Time: The Critical Importance of Risk Management in Defending Against Zero-Day Attacks

A Conversation with Top Financial Services CISO Steve Katz

For the last decade, commercial and government organizations have battled a steady stream of computer worms, viruses and other malicious code attacks. And while few large or mid-sized outfits have been put out of business as a direct result of these exploits, billions of dollars each year are lost to clean-up costs, missed business opportunities, brand/reputation damage and halted productivity. The median corporate impact of 2003's Blaster worm alone was \$475,000¹.

Now for the *really* bad news: A new and particularly dangerous threat may soon cause us to remember this period as "the good old days." That threat is the recent "zero-day" attack, so named because it leaves you absolutely no time to prepare a defense in advance of an attack.

Developed specifically to exploit software vulnerabilities during the period before patches, signatures and other fixes are available, zero-day attacks are not recognized by traditional security products: they enter your network undetected and quickly jeopardize your informational assets as well as your bottom line.

A Matter of Timing

During his tenures as chief information security officer (CISO) at J.P. Morgan, Citigroup and Merrill Lynch, noted security expert Stephen R. Katz, CISSP stared down the barrel of a never-ending barrage of cyber-attacks launched against the financial services industry. Now president and founder of Security Risk Solutions and an executive advisor to Deloitte, Katz knows well the critical importance of risk management in mitigating the potentially enormous damage that can result from an attack for which there is no immediate defense.

"It used to be the case that the creation of worms, viruses and other cyber-attacks lagged behind the discovery of vulnerabilities by 50 to 180 days," says Katz. "But lately, we're seeing that the time it takes to exploit a vulnerability is shrinking much faster than the time required for software manufacturers and security vendors to become aware of that vulnerability and create and distribute a fix. Zero-day

"When you apply [a classic risk management framework] to the zero-day threat, you quickly begin to realize why prevention is the holy grail of risk management,"

attacks – where the attack comes before a vendor is made aware of the vulnerability or before a fix is prepared and released – are the ultimate sign that the gloves are off when it comes to launching strikes against corporate networks."

To put an even finer point on the risk presented by zero-day attacks, Katz offers a real-world timeline for the development – and subsequent installation – of patches for most newly discovered security vulnerabilities. "Typically, what you see is that it takes weeks to months after notification of a security vulnerability for a vendor to develop a patch. It then takes most organizations another 20 to 45 days to test and install the patch, starting on high-value assets and systems and then moving on to lower-priority areas. So the total amount of time between vendor discovery of a vulnerability and customer installation of patches can range from 45 to 120 days. Unfortunately, during this time, additional attacks keep coming and many organizations become overwhelmed and never get past that first step of protecting their high-value assets," says Katz. "Even in the best of circumstances, it's still weeks to months before you

¹ TruSecure/ICSA Labs

have fully deployed a patch. However, you now have this block of time where the vulnerability is out there, people know about it, and you're totally unprotected."

At least in those cases, organizations are aware of – if not immediately protected from – a known vulnerability. "With zero-day attacks, the exploit can hit your network before you even know about the vulnerability," adds Katz. Given that the more time the malicious code from a zero-day attack remains active in your network, the greater the potential damage, it's easy to see how a zero-day attack could wreak untold havoc if not quickly contained and neutralized.

"Immediate, accurate detection and containment is the only effective way to prevent zero-day attacks from causing widespread infection and damage,"

Understand the Threat, Manage the Risk

According to Katz, a classic risk-management framework is effective for making decisions on how best to deal with worms, viruses and other malicious code.

"This involves taking an inventory of all the network assets you need to protect and asking yourself a sequential series of key questions," he says. "Once you've identified the items and areas you want to protect, the first question is: 'Can I possibly prevent an attack?' If the answer is 'no,' the next question is: 'What tools and technologies do I need to have in place to detect the attack when it occurs?' Next up is: 'When I detect the attack, what tools, technologies and processes do I need to have in place to contain it?' Following that question is: 'Once I've contained an attack, can I launch an investigation in order to determine how, when and why the attack occurred?'" Finally, says Katz, those charged with protecting corporate networks and assets must ask: "How do we recover from this attack and reconstitute our systems back to their normal operating state?"

"When you apply that line of questioning to the zero-day threat, you quickly begin to realize why prevention is the holy grail of risk management," says Katz. "The time and costs required to prevent an attack are nearly always significantly less than those required for investigation, clean-up and recovery once an attack has occurred."

When All Else Fails

With cyber-attacks on the rise, most commercial organizations have wisely implemented a multi-level security approach that relies on a variety of technologies to thwart or mitigate attacks. However, even today's most sophisticated security products leave your network vulnerable to zero-day attacks. Here's a sampling of current technologies and the myriad reasons they fall short in the face of the zero-day threat:

- **Network Intrusion Prevention Systems (IPS)**

Fundamentally an in-line perimeter defense, IPS cannot prevent or contain internal attacks. And because this methodology relies on vendor-supplied signatures, your network is defenseless against zero-day attacks until new signatures are developed and deployed.

- **Host-Based Systems**

Difficult installation, significant maintenance, and the need for a unique product for each OS and application within the network environment make host-based solutions expensive and impractical to deploy across an entire network.

ZERO-DAY ATTACKS

- Computer worms, viruses and other malware that target new or undisclosed security vulnerabilities for which patches and other fixes have yet to be developed.
- Called "zero-day" because they leave you no time to prepare a defense.
- Can come from external sources or be unwittingly unleashed within the network perimeter.
- It can take up to 120 days for the development, distribution and subsequent deployment of patches and fixes.
- The only effective defense is an immediate, accurate and automated response that detects and contains attacks.

- **Network Behavior Anomaly Detection (NBAD)**

By not offering fully automated responses and failing to recognize attacks until significant infection and damage have occurred, NBAD solutions leave a serious hole in your network security approach.

- **Patch Management**

While it is important to observe sound patch management practices, even the most up-to-date patches cannot protect your network against zero-day attacks, which, by definition, exploit security vulnerabilities for which patches do not currently exist. As with IPS solutions, your network is defenseless until new patches are developed and deployed.

“Sitting around and praying for a patch to arrive just won’t cut it. You need immediate, automated protection...and not just at the network perimeter.”

Closing the Gaps, Quickly and Accurately

So, how can your organization close the gaps left by the above technologies and more effectively manage the zero-day risk? What currently available products can deliver the “holy grail” of prevention to which Katz refers?

“Because attacks can come from both external and internal sources, immediate, accurate detection and containment is the only effective way to prevent zero-day attacks from causing widespread damage,” says Katz. “Sitting around and praying for a patch to arrive just won’t cut it. You need immediate, automated protection...and not just at the network perimeter.”

Enter products such as CounterStorm-1, an integrated suite of network security appliances from CounterStorm, Inc. CounterStorm-1 detects and contains attacks in seconds, allowing for “business as usual,” even during zero-day attacks. By immediately and accurately detecting and neutralizing zero-day attacks without the need for signatures or patches, CounterStorm-1 succeeds where other technologies fail, and all without fear of lost productivity from false-positive results. Its ease of integration, deployment and management also provides a distinct advantage over other technologies.

“When you’re reacting to a zero-day attack, every second counts. CounterStorm-1 gives you the confidence of knowing that those precious seconds won’t turn into hours, days, or weeks.”

In the End, It’s All About the Business

For today’s technology-dependent companies, managing the risk of zero-day and other cyber attacks comes down to protecting the business environment. And while the most important asset any company has is its trusted relationship with its customers, preserving your hard-earned reputation is only one factor driving the need for sound risk management practices. A significant amount of legal and regulatory pressure is forcing companies across a wide variety of industries to ensure that customer data is adequately protected. This includes the Sarbanes-Oxley (SOX) Act, the Health Insurance Privacy and Accountability Act (HIPAA), the Gram-Leach-Bliley (GLB) Act and other regulations from such federal agencies as the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC).

“We’ve seen a number of instances lately where customer data has been stolen, leaked or otherwise compromised,” says Katz. “That’s why smart, proactive companies will deploy a product like CounterStorm-1 to strengthen their current network security investments and add an extra layer of security to high-value and mission-critical information assets.”

And as with most aspects of the business world, says Katz, time is of the essence. “When you’re reacting to a zero-day attack, every second counts. CounterStorm-1 gives you the confidence of knowing that those precious seconds won’t turn into hours, days or weeks. That’s risk management in action, particularly in this era of the zero-day threat.”