

PROCESSOR

Products, News & Information Data Centers Can Trust

Sign Up For A
FREE SUBSCRIPTION! >>>>

Home | Register | Contact Us

**Total SMB
Data Center
Solutions**

www.stacoenergy.com



**STACO
ENERGY**
PRODUCTS CO.

This Week's Issue

Browse All Issues

Search All Articles

Product News & Information

Company
News & Information

General Feature Articles

News

Opinions

[Email This](#)
 [Print This](#)

Tech & Trends

General Information

June 4, 2010 • Vol.32 Issue 12
Page(s) 34 in print issue

Proactive Counter-Hacking Security Solutions

Identify Risks & Threats, Develop Targeted Defenses

IT has historically treated security like homeowners in a crime-riddled neighborhood who add so many dead bolts and window bars, their houses look like Fort Knox. The armored exterior looks safe but provides a false sense of security as clever burglars eventually find ways around the fortifications. Likewise, security professionals now realize that passive security measures are of limited effectiveness against professional hackers and their powerful financial incentives. Although "active defense" is a seeming oxymoron, as banks learned long ago, security is more effective when passive techniques, such as vaults, are supplemented with active measures such as security guards.

Of course, proactive measures are not cheap, can't be fully automated, and require research to find your highest risks and biggest threats. In addition, some techniques, such as white hat or ethical hacking, which mirror those of the hackers you're defending against, can pose ethical or legal risk. Yet, according to Paul Sop, CTO of Prolexic Technologies (www.prolexic.com), a network security services firm, anyone doing significant business over the Internet must augment traditional security techniques with more aggressive measures.

■ Start With Risk Analysis

Key Points

- Proactive security entails identifying your most important information assets and the security risks for each, gathering threat intelligence, and designing targeted defenses for each.
- Professional cybercriminals are skilled at evading conventional security measures, so a defense program must include continuous, active monitoring of sensitive applications, systems, and networks.
- Proactive measures center on people and processes; however, security software technologies are emerging that can detect threats and adapt their defenses in real time.
- A proactive strategy may

A proactive strategy starts by identifying your digital crown jewels. According to Jeffrey Carr, security consultant and author of “Inside Cyber Warfare,” “The first thing to do is an assessment of what’s valuable. You clearly can’t protect everything from everybody, so your resources, including financial, should be dedicated toward protecting the most valuable assets.” A strategic shift from blanket-edge security to targeted defenses is also recommended in a report by Deloitte’s Center for Security and Privacy Solutions: “One of the more fruitful approaches to consider in addressing the threat of cyber-crime involves moving from a primarily security-based approach to a more risk-based approach.”

prevent many attacks and render others less effective; however, counter-attacking the perpetrator is illegal cyber-vigilantism in most jurisdictions. Even putatively safe realms for counter-hacking or clandestine surveillance—on employees, for example—can be legally risky and a violation of corporate policies.

Just as physical surveillance is the cornerstone of real-world security, so, too, is proactive monitoring of the IT infrastructure a requirement in the cyber world. Perhaps Mark Twain put it best when he wrote, “Put all your eggs in one basket and—watch that basket!” Sop recommends enterprises first deploy an anomaly detection system that benchmarks a network’s normal behavior. He adds that this is increasingly difficult because sophisticated attacks now use various tricks to fly under the radar of conventional IDS systems. Carr agrees that professional attackers take pains to act in ways that avoid detection but aren’t infallible. “Look for things like an employee that shouldn’t be an administrator who now has administrator rights, or an employee who would normally be accessing a particular file or project a few times a week who is now in there an hour at a time every day.”

■ Mount An Informed Defense

Having established an active monitoring regime, Carr says the next step is to gather intelligence on who might want what you have. This often comes down to someone looking for a competitive advantage by stealing intellectual property or secret plans. “For example, one of the priorities in China is the smart grid and developing cheap energy,” says Carr, so, “if you happen to be in that business, then you can count on having your valuable information targeted by agents who think there’s a market for what you have.”

Deloitte’s report describes intelligence gathering as a continuous scouting expedition using various sources for information about the threat environment, whether industry groups such as the various CERTs (computer emergency response teams), law enforcement, or security vendors. Other techniques include creating honeypots to trap probable hackers or monitoring hacker forums, although this can be tricky because the black hats are vigilant in detecting poseurs.

Next, you’ll want to use threat intelligence to develop an informed defense strategy, according to Carr. He likens this to a football coach using recordings of the opposing team in designing a game plan: “Once you know who you’re dealing with, you can organize an appropriate defense.”

The tactics often entail adding personnel or security services and enhancing procedures. “There is no silver bullet,” says Prolexic’s Sop; however, active, adaptive technologies are also making their way into new security appliances. David Koretz, president and CEO of Mykonos Software (www.mykonossoftware.com), says there’s a gaping hole in the typical security measures for Web applications. Firewalls and client-side scanning only detect attacks after they’ve succeeded, he says. “It’s equivalent to having a fire alarm after your house burns down,” he adds.

■ Corporate Policies & Counterattacks

An aggressive security strategy should include risk analysis, threat intelligence, and an active, adaptive response to attacks, but a counterattack is clearly off-limits. “There is no

right of self-defense,” says Carr. “It would clearly be an illegal act and the Justice Department would be entitled to prosecute a U.S. company that engaged in attacking another network.” As he summarizes in his book, active counterattacks on cyber criminals is the province of governments, not individuals or enterprises.

Even when attacks come from insiders, hacking the hacker is risky. And the question of whether digital employee surveillance violates the employee’s right to privacy is also a legal gray area and is currently the subject of a Supreme Court case. ■

by Kurt Marko

Active Web Application Security Techniques

Code-level modification and data protection: Security appliances or proxies can inject a layer of confusion and misdirection into existing Web applications, making it harder for hackers to introspect and discover vulnerabilities.

Identify and track hackers: Pinpoint hackers and security incidents as the attack occurs and enable application administrators to track activities over time.

Gain hacker intelligence: Gain an understanding of hacker behavior using technology that profiles their capabilities, evaluates skill levels, and classifies the threat they pose.

Establish counter-measures: Once the skills of the hacker are classified, security administrators can decide on the appropriate response or counter-measures to deploy in real time. Counter-measures can also be defined and executed based on policy.

Analyze attacks over time: Drawing upon a database of known hacker behaviors and analysis of Web application attacks over time, gather intelligence to understand the real exposure and to better anticipate and prioritize responses against future attack scenarios. The more the hacker is understood, the better prepared an organization is to deal with future security incidents.

SOURCE: MYKONOS SOFTWARE

Share This Article:

