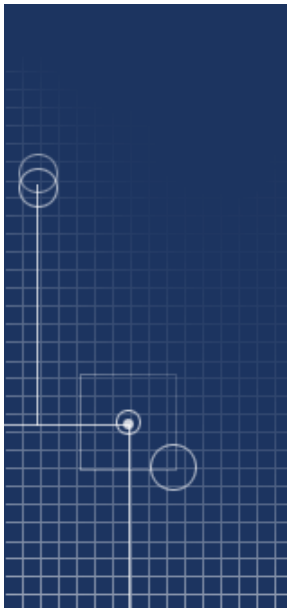

Cover Focus Articles

General Information
July 16, 2010 • Vol.32 Issue 15
Page(s) 10 in print issue

Today's Biggest Security Threats

Danger Could Be Just Around The Corner If You Don't Stay Abreast Of New Issues

At a time when threats against enterprise infrastructure are increasing like never before, IT security decision makers are challenged by the rapidly changing nature of these threats. Using conventional tools and processes to protect the perimeter is no longer enough as applications and data migrate to cloud-based and mobile platforms. IT shops that aren't rethinking the threat environment are leaving themselves unnecessarily vulnerable.

Traditional firewalls, for example, are unable to keep pace with new forms of attack that target applications instead of operating systems and hardware. The gradual migration of enterprise functionality outside the firewall only adds to the challenge.

"Social media, blogs, wikis, video, mobility, AJAX, and file sharing are just a few of the Web 2.0 applications that are commonly used, yet not secured by traditional firewalls," says Jonathan Hoppe, president and CTO of Cloud Leverage (www.cloudleverage.com). "In addition, DDoS threats and botnets become more prevalent all the time and can cripple traditional firewalls with limited capacity."

Clouds In The Forecast

Cloud-based solutions, in particular, are pushing the bounds of conventional security methodologies.

"This technology has proved incredibly valuable to enterprises worldwide in managing capacity, but because of the fact that it resides outside of corporate firewalls, it is very difficult to protect," says Hoppe, who adds that as cloud-based

Key Points

• Traditional firewalls are becoming inadequate as a growing percentage of corporate IT resources rely on the Internet and cloud-based resources.

• Increasingly capable smartphones open up new avenues for security vulnerability, meaning conventional management tools and processes—built for traditional PCs—are inadequate.

• Employees using social media can make it easy for hackers to target individuals with customized spearphishing attacks or to use the employees' information to spread malware and build botnets.

implementation continues its mainstream push, enterprises will look to cloud-specific IPS and firewall solutions as a second layer of protection.

Behaviors also continue to rank high as potential security weaknesses. Unfortunately, insider threats are often mistakenly overlooked by outward-focused IT security leadership. Terry Cutler, a premium services engineer with Novell Canada (www.novell.com), says end users in many organizations are typically given too much access for their respective roles. Even if their subsequent explorations aren't malicious, Cutler says they can represent the most significant threat to the organization. And if they are malicious, employees using this data for alternative purposes can damage the organization's bottom line and credibility.

More Mobile, Less Controlled

As more mobile devices—often purchased by employees instead of procured centrally through IT—connect to corporate infrastructure, the risk grows. Employees typically have much greater control over installing and configuring apps on mobile devices than on average IT-managed corporate PCs.

"Consumers are also increasingly accessing the Internet on these devices to check bank balances and conduct e-commerce transactions," says Ansh Patnaik, director of industry solutions at ArcSight (www.arcsight.com). "In other words, smartphones are approaching desktops in terms of value to cybercriminals while protection measures are much weaker. That's why many experts predict that mobile malware will hit hard this year."

The increased need for employees to self-manage Internet-based resources—functionality that was once IT's exclusive domain—increases the potential number of incursion points.

The Rise Of Anti-Social Media

Greater use of social media tools at all levels of the typical organization also spells bad news for IT security. Hackers are locking in on rising rates of participation in services such as Twitter and Facebook to build customized "spearphishing" attacks. Cutler cites an example of employees attending a conference who tweet that they're glad to be home. Hackers could then use that information to email them a link to pictures taken at the event. The potential for click-through is much higher because it doesn't seem to be coming from a stranger.

Cutler says this is representative of new styles of attacks where a hacker uses detailed information about his target to improve his odds for success by crafting a compelling email message and Web page. The social media threat also extends beyond socially engineered attacks.

"Cybercriminals are leveraging the socially viral nature of these networks to spread malware and convert hosts into bot zombies," says ArcSight's Patnaik. "The continued increase in the use of social networks at work makes Internet-facing desktops inherently vulnerable and a conduit for cybercrime."

Threats Get Quieter

The nature of attacks is also changing. Gone are the days of big-bang incursions. The TJX data breach that exposed more than 45 million credit and debit card numbers went undetected for well over a year.

"We used to know when bad things were happening because it'd be a major network event, such as outages, failures, [or] traffic spikes," says Matt Jonkman, founder of Emerging Threats (www.emergingthreats.net), an open-source community project that creates intrusion detection signature and rule sets. "Unfortunately, now the attackers intentionally stay extremely quiet. The pain will come in the infections that have been resident for weeks or months. Recovering from these breaches and identifying the information and credentials that may have been compromised is a herculean task."

Preventing those breaches in the first place is especially critical as the need to protect confidential customer and stakeholder data continues to escalate. CDW's most recent Threat Prevention Straw Poll highlights data loss as the main threat that's attracting most

organizations' focus.

"Data loss is possibly the biggest security-related threat," says Stan Oien, manager of security solutions for CDW (www.cdw.com). "Whether it is from parties inside the organization maliciously taking or destroying information or simply broken operational processes that lead to data loss through negligence, the threat is real." ■

by Carmi Levy

New Forms Of Data Present New Vulnerabilities

As federal stimulus funds work their way through industries such as health care and utilities, they may be creating new categories of data that are especially ripe for attack.

"Medical identities carry a huge premium over other identities such as credit card numbers in the black market and will increasingly be targeted with old and new threats as they are digitized and used on the Internet," says Ansh Patnaik, director of industry solutions at ArcSight (www.arcsight.com). "Similarly, SmartMeters are being deployed at millions of homes and businesses [to closely monitor electricity usage] and introduce new opportunities for cybercrime as well as cyberterrorism."

IT must categorize and protect these emerging forms of data to stay ahead of the evolving threat curve.

Return to Previous Page