



KPMG ANALYSIS

Data Protection Takes Center Stage in Network Security

February 16, 2007
By Dave Pelland, Managing Editor, Technology Insider

As information security threats emerge faster than traditional methods can contain them, companies are adopting an "info-centric" approach to security based on protecting data, not just restricting network access.

"For too long, security has focused on the [network] perimeter and not on protecting the information itself," said Art Coviello, president of EMC's RSA security division, at the RSA Security Conference in San Francisco.

"It's like we've protected the moat and the castle, when we should have protected the king," Coviello said. "Static solutions are not enough for dynamic attacks. We need an inside-out approach to security that's based on [protecting] the information itself."

Emerging approaches to security are a generational shift from methods that relied heavily on signature-based products such as anti-spyware and intrusion-detection software to detect previously identified threats. Instead, enterprises are turning to encryption, pattern-recognition software and other technologies to safeguard data as they link the protection of information to their business strategies.

"Security can't be a tactical afterthought or a technology that's bolted on as a defense," Coviello said. "Security can do more than protect the business -- security can accelerate the business."

Different approaches to network security have evolved because the threats are getting worse. Sam Curry, vice president of security management for CA, says that instead of the stereotypical teenage hackers erasing data or defacing Web pages, professional crooks are launching high-quality attacks that harvest data sold to identity thieves or use corporate servers to relay spam.

"Malware is constantly evolving," Curry says. "It's becoming more professionally produced and it's designed to resist detection and steal personal or corporate information.

"This isn't vandalism motivated by notoriety -- once this stuff gets on PCs, it's designed to stay there as long as possible. These attacks are motivated by money, and the more systems hackers can control, the more money they can collect."

Eugene Kaspersky, head of research for antivirus provider Kaspersky Lab, said that targeted attacks are often designed to sneak onto a single corporate network or server. The number of malicious software samples Kaspersky Lab examined in 2006 increased threefold from 2005.

The evolving threats mean companies are trying to ensure information is kept safe from unauthorized access while remaining available to those who need it. For instance,

MORE...

Attachment Spam May Emerge as Malware Vector

AUGUST 8 PDF attachments are the latest effort to evade corporate spam filters, and may foreshadow the use of e-mail attachments as a way to deliver malware.

Selected Technology Company Earnings

JULY 31 Technology and media companies generally reported earnings growth in the second quarter.

Transfer Pricing Risk Hitting Boardroom Agendas

JULY 25 Technology companies face a major challenge in transfer pricing risk as national governments seek new sources of tax revenue.

Product Placement Takes Its Role on the Global Stage

JULY 18 The head of a television studio talks about how product placements are expanding across the globe.

Data Protection Gets Policy, Tech Backing

JULY 11 The focus of enterprise security is shifting to data protection and stronger policies for accessing and storing information.

IT Governance Is a Matter of Information Over Technology

JULY 5 A language barrier between audit committee members and technology officers can severely complicate IT risk oversight.

For Better Security, Web Browsers Go Green

JUNE 26 The latest generation of Web browser certificates could help reduce phishing attacks against banks, retailers and other companies.

companies are encrypting data stored on servers, which helps reduce the chance of the organization being compromised if an attack hits.

Enterprises are also encrypting e-mail messages that enter and leave the organization. If an outbound e-mail appears to have sensitive information, the message can be encrypted or even blocked at the message gateway.

"Even if the corporate perimeter is breached, which unfortunately does happen, the attack is much less effective if the data is adequately encrypted and can't be rendered," says Greg Porter, a Pittsburgh-based manager in KPMG's IT Advisory practice.

Better end-user education about information security is also expected to protect computers and networks, according to John Thompson, chairman and CEO of security provider Symantec.

Thompson said security firms need to give users better information about Web sites as they connect. This can involve adoption of one-time-use credit cards to prevent accounts from being stolen after a transaction is completed; giving users better information about a Web site's certificates to validate identity information; and providing third-party information about a site's reputation and business practices.

"Users need better tools to challenge the sites they do business with," Thompson said. "The need to protect identities today dictates that we help our customers with better information about sites, security and reputation."

EMC's Coviello said technologies such as pattern-recognition software that monitors network traffic and establishes a baseline of normal activity have made network defenses more dynamic. This is expected to give companies the ability to detect abnormal behavior on the network, such as the installation of spyware or other unwanted malicious code.

For instance, an online banking customer logging in with a computer they've used before could be granted access with just their password and by recognizing an image displayed on their screen. But that customer would have to answer a series of security-related questions if he or she deviates from their normal usage patterns, such as by using a different PC or logging in from outside their home country.

Some companies are exploring so-called "white list-" based approaches that specify which applications will be allowed to run on the network. Unlike anti-virus or intrusion-detection software that identifies programs as malicious (using a "black list" of known threats) and prevents them from running, white list programs will only allow approved programs to run.

"Security is less about what the widget of the week is -- it's more about a philosophy that gives companies the confidence that their IT systems and data are secure, and can be reached only by those people who should be reaching them," says CA's Curry. "If there's not a business reason for someone to access some data, that access needs to be turned off."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

Submit

© 2007 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative. All rights reserved.

[KPMG Online Privacy Statement and Disclaimer](#)