



KPMG ANALYSIS

Web 2.0 Opening Doors for Content and Threats

April 17, 2008

By Dave Pelland, Managing Editor, Digital Insider

The growing enterprise use of consumer-oriented Web 2.0 tools such as social networking sites, blogs and wikis promises to increase corporate productivity, but their collaborative nature could also expose networks to a host of Web-delivered security risks.

"We are re-architecting the way we interact with Web sites," said Ed Skoudis, co-founder of security consulting firm Intelguardians, at the RSA Conference 2008 in San Francisco. "Rather than viewing static content, we're opening sites so you can create content and post it. We have millions of users posting content for millions of other users. But what if the content someone posts on a site is malicious?"

The reliance of Web 2.0 sites on content contributed by users, for instance, means hackers can post malicious scripts that compromise their computers, or links to sites that distribute software code designed to steal corporate or personal information such as keystroke loggers, or could enlist an infected computer into a botnet (a remotely controlled network of machines used to relay spam or for phishing attacks).

In many instances, malicious content is added to the Web sites of legitimate companies, which infect employees and outside users without knowing they've been compromised.

"When you start a Web browser, you start it from inside the firewall, and if you visit a Web site with hostile intent, the code is able to come back through the firewall and have a shot at executing," says Roger Thompson, leader of the research group for security software provider AVG.

The threat of Web-delivered malware is considered especially dangerous for enterprise networks because the malicious code typically looks like normal Web traffic, which corporate firewalls are programmed to let in.

In response, more companies are starting to add software that performs real-time scanning of Web pages to their network firewalls to check Web-based content as it's downloaded. Companies are also scanning links suggested by search engines to determine if the links are pointing to hacked sites hosting malicious content.

"A Web page may be assembling content from 50 other sites. We can let the safe content render and block the malicious links," Thompson says.

Thompson says security pros also benefit from the fact that attackers tend to recycle malicious code and methods by using automated malware creation tools, which gives

MORE...

[IFRS for Technology Companies: Closing the GAAP?](#)

AUGUST 14 A KPMG white paper examines industry-specific issues for technology companies considering a transition to International Financial Reporting Standards.

[The Consumer Electronics Boom](#)

AUGUST 6 A new KPMG white paper identifies the critical issues inhibiting faster time-to-market for consumer electronics and semiconductor manufacturers.

[Wireless Carriers Put Money in Mobile Banking](#)

JULY 29 Cell phone carriers are targeting mobile banking applications for growth.

[Selected Technology Company Earnings](#)

JULY 25 Slowing economic conditions in the United States affected the results of several technology companies in the second quarter.

[Companies Taking Green-Tinted Look at Data Centers](#)

JULY 18 As corporations become more environmentally aware, they're looking at their data centers and PCs to reduce energy consumption and carbon footprints.

[Social Media: a New Political Animal](#)

JULY 10 Social media is reaching beyond the traditional corps of political pros and playing a major role in the fall elections.

[KPMG's Quarterly New and Emerging Markets Magazine](#)

JULY 2 In this issue, KPMG examines how the wireless revolution is shaping everyday life in emerging markets to its logistic systems.

researchers clues to look for and make detection somewhat easier. By searching for known hacker delivery methods, researchers can assume incoming code is malicious.

"All of the antivirus companies are getting 20,000 to 30,000 samples a day, but they're all being delivered by the same 100 to 150 Web tricks," Thompson says. "It's like sending people letter bombs but writing on the outside of the letter, 'I'm a bomb.'"

Blocking Not Practical

The traditional IT response of blocking new tools until they're proven to be safe is wavering in the face of Web 2.0. The emerging popularity of social networking tools in the workplace, for instance, makes it difficult for employers to deny their use.

"We're seeing a greater consumerization of IT and the enterprise," said Mark Bregman, chief technology officer of security provider Symantec. "Employees today know how to do computing because most of them grew up with it. New technologies are sneaking into the enterprise and in many cases are bypassing IT, and then IT has to accommodate them. This is generating new [security] challenges.

Patrick Heim, chief information security officer of Kaiser Permanente, said that with more employees working outside traditional hours or locations, security professionals have to confront growing demands for additional flexibility.

"When you're trying to recruit the next generation of individuals to work in a large organization, locking down devices and the network sends a tone that may affect your ability to attract talent," Heim said. "We need to be careful as security individuals because there may be downstream impacts on our organizations if we try to tighten down too much."

Focusing on Information

The growing attention to Web-borne threats is part of a shift among corporate security pros away from trying to secure the perimeter of the network --toward protecting information, whether it's stored on the network or on users' portable devices.

"In the past, our reaction [to emerging threats] would be to build higher walls or stronger walls, said John W. Thompson, chairman and CEO of Symantec."But today we can't do that and have a successful business. Decision making depends on access to real information, so we must rethink our approach to security."

For example, Thompson said companies are turning to stronger identity-based controls that dictate the types of information workers can access and what they do with it. For instance, some workers may be allowed to read e-mail messages, but not to print or forward those messages. Similarly, some workers may be blocked from copying sensitive files to portable storage devices. "Information-centric security is about taking a risk-based approach toward protecting confidential information," Thompson said. "With the amount of stored data growing 50 percent per year, trying to protect it all is both inefficient and costly. Instead, it's about securing the most critical information."

Val Rahmani, general manager of IBM's Internet Security Services unit, said companies are turning away from relying on separate products to address specific threats, such as specific appliances to examine incoming traffic for viruses or spam

messages, because new threats emerge too quickly for such tools to be current and effective.

Instead, more companies are adopting tools that monitor the normal operating conditions of a network and look for behavior anomalies that may be caused by malicious code.

"Having a point product for everything isn't going to solve this, because there's always going to be a smart hacker who finds a way though all of the tools," Rahmani said.

"We have to think about this holistically and assume that everyone's infected?we have to start treating the root cause of the problem, not just each symptom as we find it."

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](#)

© 2008 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

[Privacy](#) | [Legal](#)