

Meeting the Challenge of Today's Blended Threats

Cyber-crime and its costs are increasing rapidly.

The FBI received a record number of complaints in 2008, and the associated direct cost of the frauds carried out with stolen data was \$265 million, up about 11 percent over 2007.

There is no sign that this trend will abate. Last year's growth and today's continuing problems can be attributed to one fact: Hackers are becoming more sophisticated in their efforts to steal personal identity data and sensitive corporate intellectual property. In particular, they are increasingly using socially engineered, multi-pronged, and blended attacks that exploit the openness of Web 2.0 applications and Web sites.

Compounding the challenge of securing personal information and intellectual property data is that companies are being forced to grant access to more systems and information all the time. Bank customers want quick access to account balances, workers want to maintain their own 401k and health insurance accounts, Web shoppers want to place orders quickly and make purchases with a single click, and business partners want to work on projects in a collaborative manner online.

Additionally, companies are increasingly using SaaS (software-as-a-service), which means employees must go online to access corporate applications.

Companies naturally benefit from the customer and worker satisfaction of this openness afforded by Web 2.0 and self-service approaches. But, as expected, the openness brings additional risk.

Changing hacker tactics

Security has always been fighting to keep up with evolving tactics. Current-generation hackers seem to be raising the stakes to even higher levels.

First, hackers are using multi-pronged, blended attacks. A typical scenario includes sending a spam e-mail that tries to lure the recipient to a Web site. That site might be poised to download malicious software as soon as the user connects to the Web page. That software often includes a keylogger program that steals passwords, malware that steals application data, or a program that turns the computer into a remotely controlled bot that can be used to launch denial-of-service attacks, distribute spam, or spread other malicious code. Alternatively, the landing page might be a replica of a legitimate site, such as a banking or e-commerce site, whose purpose is to trick the user into giving up account information.

Second, attacks are more targeted and use more sophisticated social engineering techniques to trick even savvy users into making a mistake. In the past, a phishing attack might involve sending a generic spam e-mail message (e.g. there's a problem with your eBay order, or, a Nigerian philanthropist needs help sharing his wealth) to any address the hackers had obtained. Many of these messages were easy to identify as bogus.

Now, many attacks use current-events issues or hot-button topics to trick people into taking action. For instance, hackers quickly seized on the concerns about swine flu and used phishing attacks that exploited these fears to try to steal information or sell pharmaceutical products.

And earlier this year, a spam campaign lured people to a fake, but realistic-looking, Barack Obama Web site that carried a breaking news story about Obama refusing to be president, claiming he was not ready for the position. Clicking on the link automatically downloaded spam bot software to the victim's PC.

More sophisticated attacks use information about the target to customize the phishing e-mail message, making it harder to dismiss, and, in some cases, making it appear legitimate. For example, knowing the name of a person's boss, a hacker can send an e-mail claiming, "Your boss gave us your contact information." And because some messages appear to come from friends or colleagues, the recipient usually trusts the contents.

This can cause the recipient to take action such as opening an attachment or going to a Web site—actions the recipient would possibly have avoided if the message lacked that level of detail. Oftentimes, the personal touches that make these messages more believable come from stolen information. This type of attack is essentially a more elaborate blended attack.

Third, hackers are leveraging social networking's popularity, taking advantage of users' openness and people's willingness to share information in their "communities." As noted above, socially engineered attacks often rely on information about a target to make the attack harder to dismiss and more refined. Today's Web 2.0 and social networking sites make incredible amounts of information freely available. And they often build an unjustified, but strong level of trust from "friends" in a community.

For example, in May, *The New York Times* reported on a worm-like phishing attack targeting Twitter users. The users got a message that appeared to be from a friend and implied the user could get more followers by clicking on a link. Those who clicked on the link were taken to a rogue site that looked like Twitter, which prompted users to enter their account information. That information was then used to send the same message to all of that person's Twitter followers.

Facebook has also been subject to a number of phishing attacks. In May, Reuters reported on a Facebook phishing attack that stole users' passwords. And last year, hackers sent e-mail messages that looked like they had been sent by a Facebook friend. Again, the familiarity or appearance of the message being sent by a trusted source caused people to click on an embedded link, which downloaded a virus onto the user's PC.

And fourth, hackers are using more sophisticated technologies, such as cross-site scripting, SQL injection, and frame hijacking that can be exploited because of Web 2.0 capabilities.

Some of these attacks lead a user to a rogue site. For instance, a very easy exploit is to embed a shortened URL in a Twitter update, Facebook posting, or e-mail message. Such shortened URLs hide a site's true domain name, thus giving the user no clue as to its nature.

Other attacks turn legitimate sites into dangerous territory. For example, an automated form of SQL injection attack using botnets compromised more than 500,000 Web sites last year, according to a report from the Web Application Security Consortium.

The purpose of the attacks varied, but many involved the theft of sensitive information and planting of malware. One disturbing finding was that the hackers were increasingly targeting a site's customers rather than the sensitive information in the site's database.

“While the initial attack vector was SQL Injection, the overall attack more closely resembles a Cross-Site Scripting methodology, as the end goal of the attack was to have malicious JavaScript execute within victims’ browsers,” according to the report. “The JavaScript calls up remote malicious code that attempts to exploit various known browser flaws to install Trojans and keyloggers in order to steal login credentials to other Web applications.”

Implications become more ominous

The changing tactics of hackers simply mean they now have multiple conduits into a company’s systems and data.

Unfortunately, the consequences of a breach or data loss are increasingly severe.

Data theft and breaches from cyber-crime may have cost businesses as much as \$1 trillion globally in lost intellectual property and expenditures for repairing the damage last year, according to a survey of 800 CIOs conducted by Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS) and McAfee.

On the personal information side of the equation, companies that collect and store data about their customers are subject to an ever-growing number of data privacy and protection laws and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

Some recent examples put the scope of the financial penalties imposed by regulators for breaches into perspective.

Earlier this year, credit card processing services company Heartland Payment Systems reported malicious software had compromised card data that crossed its network. In May, the company reported that the breach cost the company about \$12.6 million, including legal costs and fines from MasterCard and Visa.

In February, CVS Caremark’s pharmacy chain agreed to pay \$2.25 million to resolve Department of Health and Human Services allegations that it violated HIPAA laws.

Beyond fines, breaches carry additional financial consequences.

In most cases, when personal information is compromised, the company pays for a credit card monitoring service for one or two years for all parties impacted. Such services typically cost about \$100 per person per year. So a breach involving even a small number of customer records, 500 for example, could cost a company up to \$100,000 for two years of coverage. Breaches that involved thousands of customers can result in millions of dollars of charges.

Other costs that must be covered are any customer losses due to the fraud committed by the hackers. The FBI reports that the average individual loss last year from cyber-crime was \$931. Again, this can quickly add up to a significant expense for a breach.

Additional costs to factor in include lost worker productivity from downtime caused by malicious software and time lost to removing malicious software. Soft-dollar losses to consider are reduced customer confidence and damage to the company’s reputation. These may lead to a loss of business or revenues.

An attack may also corrupt corporate data and files. The IT staff will have to dedicate time to restore data to its pre-attack state. These operational costs simply add to the cost of dealing with a breach.

What's needed?

To reduce the risk of a data breach or theft, organizations must adopt new tactics. Specifically, today's blended threats need blended defenses.

Point security solutions simply cannot handle the multi-pronged efforts of today's hackers. Companies must address e-mail and Web security along with employing a comprehensive data loss prevention strategy.

The application of multiple security techniques is required to reduce risk. For example, there must be a way to control spam and block the downloading of malicious software from poisoned Web sites.

In today's more open Web 2.0 and social networking environments, companies also need a way to defend against attacks and protect secret or sensitive data. At the same time, they must maintain a flexible and responsive infrastructure to support today's business working habits.

McAfee as your technology partner

To meet the challenges of today's blended threats, McAfee offers comprehensive solutions that provide a modular approach to security. This allows companies to mix and match the solutions that are appropriate for their business, while offering a level of integration where management is simplified and synergies can be leveraged.

In particular, depending on a company's needs, different product combinations can be used together to provide e-mail and Web security along with a data loss prevention.

For e-mail, most companies employ a variety of products including anti-virus, anti-spam, and anti-spyware solutions from different vendors. McAfee offers the McAfee Email Gateway product family to address these threats in a single, comprehensive solution.

McAfee Email Gateway appliances deliver total e-mail protection for enterprises, integrating comprehensive inbound threat protection with outbound data loss prevention, advanced compliance, robust reporting, and administrative empowerment. They provide enterprise-class features and flexibility to increase messaging security while reducing the costs associated with spam, bandwidth consumption, malware cleanup, and data loss.

For those who need added protection, McAfee Email Encryption provides policy-based e-mail encryption ensuring that even recipients without encryption capabilities are able to receive and reply to secure e-mail. Applying encryption at the gateway instead of at the desktop eliminates the need for end users to determine encryption requirements, and avoids the common problem of end-users forgetting to encrypt sensitive data.

A McAfee Email Gateway Control Center appliance can be used to centrally manage multiple McAfee Email Gateway appliances.

The McAfee Email Gateway Quarantine Server appliance provides consolidated quarantine services for multiple McAfee Email Gateway appliances, relieving storage and processing workloads with capacity for up to 1.5 million messages.

To help deal with malicious Web sites, McAfee Web Gateway appliances deliver comprehensive security for all aspects of Web 2.0 traffic, whether entering or exiting the organization.

McAfee Web Gateway uses proactive intent analysis to filter out objectionable content from Web traffic, including encrypted traffic. By scanning a Web page's active content and understanding its intent or predicted behavior, the McAfee Web Gateway proactively protects against blended threats and targeted attacks that are ubiquitous in today's Web 2.0 environments.

Additional protection is offered through reputation-based Web filtering, powered by TrustedSource global intelligence. McAfee Email and Web Gateway both utilize TrustedSource, which continuously monitors and characterizes Internet traffic through a global network of more than 10,000 sensors in 82 countries.

TrustedSource's unrivaled effectiveness is a direct result of McAfee's unique view into enterprise mail and Web traffic. TrustedSource creates a profile of all activity on the Internet across multiple protocols, using this profile to detect deviations from expected behavior, potential attacks and blended threats. The system then generates a reputation score based on the behavior, history, and associations of the host. This score is incorporated into McAfee Web Gateway, enabling organizations to reject unwanted traffic before it enters the network.

For data loss prevention, McAfee's comprehensive set of DLP tools enables a company to secure all potential leaks in an organized and centralized way.

McAfee's approach enables companies to phase in a comprehensive protection strategy quickly. Starting with discovery of sensitive data, the solution assesses risk and helps define access and usage policies. Then it applies the necessary security measures and monitors continually to prevent any incidents and log all activities. These functions are delivered via dedicated appliances that handle the heavy processing duties and ensure that latency is kept to a minimum.

Through a unique Capture process, McAfee Data Loss Prevention tools monitor the network and create snapshots of all data. These can be searched easily to help administrators discover where sensitive data is, and observe how it is accessed and used, and by whom. Instead of manually combing network folders, the Capture feature delivers Google-like search capabilities to IT, making the process of identifying at-risk data quick and efficient.

Once risks are assessed and sensitive data located, McAfee helps companies set policies and manage multiple layers of security. Further, advanced Web-based management and reporting and auditing capabilities let companies define and manage policies that control how employees use and transfer sensitive data.

The solution covers applications, storage devices, and network communication protocols including e-mail, Web mail, P2P, IM, Skype, HTTP, HTTPS, FTP, wireless connections, USB devices, CD and DVD burners, printers, and faxes.

McAfee DLP tools also monitor real-time events and generate reports to support internal investigations and compliance audits. The Incident Dashboard is uniquely helpful in this regard. If a breach is discovered, McAfee's indexing and monitoring information can reveal, for example, who touched a particular document last, where it was e-mailed last week, or who downloaded what information prior to leaving the company.

Combined, McAfee's e-mail, Web, and DLP solutions offer a blended approach to combat today's blended threats.

For more information, visit: www.mcafee.com.

by Salvatore Salmone

Salvatore Salamone is an executive editor in Ziff Davis Enterprise's Strategic Content Group. He is the author of three business technology books and has been writing about science and information technology for 20 years serving as a senior editor at many major publications including Network World, Byte, Data Communications, LAN Times, and InternetWeek.