



The Milestone Review

DECEMBER 2009

inside

Protecting cardholder data ... page 3

How to fight phishing ... page 4

Use of Social Networking and Collaborative Applications Is Exploding ...

Are You Ready for the Potential Fallout?

Milestone and Palo Alto Networks deliver next-generation firewalls that enable unprecedented visibility and granular policy control of applications and content with no performance degradation.

The use of social networking and collaborative applications for business purposes skyrocketed between March and September 2009, according to a recent study by Palo Alto Networks. With increased adoption of Web 2.0 applications comes new business and security risks that reach far beyond potential productivity losses. Yet many companies have outdated IT infrastructures and usage policies that may fail to protect them. Gartner, Inc. estimates that, through 2012, enterprises that take a “block or ignore” stance toward employee use of consumer IT will incur security incident costs 2 to 4 times those of enterprises that use “embrace or contain” strategies.

What's Going On?

Unlike other industry reports that are based on behavioral surveys, Palo Alto Networks' semi-annual Application Usage and Risk Report looks at which applications are in use, identifies emerging trends, and discusses the associated business benefits and risks. Some specific findings from the Fall 2009 report include:

- Twitter use grew more than 250 percent from the Spring 2009 edition of the Application Usage and Risk Report, published in April.



- Facebook use increased 192 percent while Facebook Chat (released in April 2008) was the fourth-most commonly detected chat application, ahead of Yahoo! IM and AIM.

- Blogging and wiki editing increased by a factor of 39, while total bandwidth consumed increased by a factor of 48.

“Despite many enterprises’ attempts to block these applications, the rate at which they are making the crossover from personal to business use is happening faster

than previous crossovers, such as instant messaging,” said Tom Olson, Senior Security Engineer at Milestone Systems. “The use of social networking applications can bring measurable business benefits, but not without introducing business and security risks. These applications can transfer files, propagate malware, and have known vulnerabilities that can be exploited.”

Milestone has partnered with Palo Alto Networks to provide next-generation firewalls that enable unprecedented visibility and granular policy control of applications and content with no performance degradation. Palo Alto Networks firewalls accurately identify and control applications — regardless of port, protocol, evasive tactic or SSL encryption — and scan content to stop threats and prevent

data leakage. For the first time, enterprises can embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation.

Command and Control

Organizations are using Web 2.0 applications for cultural reasons, to improve efficiency, to foster customer intimacy, and to speed up business processes. At the same time, security technologies have retained an outmoded “block or allow” model, lacking the granularity and intelligence to recognize and appropriately control these new applications.

Traditional firewalls block or allow network traffic based on ports and IP addresses—they cannot distinguish among the many Web applications running through ports 80 and 443. However, Palo Alto Networks firewalls can distinguish particular applications within Web traffic and filter them. This allows organizations to create granular, business-relevant security policies and safely control new applications.

“Social networking and collaborative applications are increasingly considered to be Enterprise 2.0 applications. These business-enabling applications are not threats, yet they pose risks to enterprise networks,” said Olson. “Palo Alto Networks firewalls take a ‘positive’ approach to security that gives organizations the flexibility to embrace Web 2.0 applications, yet still manage risk. These solutions go beyond the outmoded ‘block or allow’ model used by many other security technologies.”

Establishing Priorities

Quality of Service (QoS) is also impacted by Web 2.0. PAN-OS 3.0, the latest version of the operating system software for Palo Alto Networks firewalls, introduces traffic shaping in the firewall, enabling enterprises to ensure that priority is given to business-critical functions. The QoS features in PAN-OS 3.0 enable organizations to shape and prioritize traffic based on application with multi-gigabit throughput due to the single-pass software married to hardware-accelerated queuing.

“According to the Palo Alto Networks’ Spring 2009 Application Usage and Risk Report, more than half of the bandwidth in a sample of actual application traffic from more than 900,000 users was being consumed by 28 percent of the applications, most of which were consumer-oriented,” said Olson. “Palo Alto Networks’ application visibility and fine-grained control capabilities offer organizations flexible policy responses to applications — including allow, deny, allow for certain users or functions, threat scanning, and now shape. Administrators are able to manage the bandwidth consumed by applications, as well as their priority — all in firewall policy — instead of simply killing applications or having no visibility or control over them.”

The analysis discovered 255 Enterprise 2.0 applications — of which 70 percent are capable of transferring files, 64 percent have known vulnerabilities, 28 percent are known to propagate malware, and 16 percent can tunnel other applications. Examples of new threats introduced to enterprise networks by applications such as Facebook include Koobface, Fbaction and Boface, which all target social networking applications to hijack accounts and personal data.

“We know that workers are using these applications to help them get their jobs done, with or without approval from their IT departments. And now we know this is happening much faster than anticipated. It’s naïve to think that old-school security practices can handle this deluge,” said Rene Bonvanie, Palo Alto Networks vice president of worldwide marketing. “Organizations must realize that banning or allowing specific applications in a black-and-white fashion is bad for business. They need a new approach that allows for shades of gray by enforcing appropriate application usage policies tailored for their workforce. This is a radical and necessary shift for today’s IT security professionals.”

The Application Usage and Risk Report is available for download at http://www.paloaltonetworks.com/literature/AUR_report1109.html. Additional information on the more than 900 applications identified by Palo Alto Networks can be found in Applipedia, part of the company’s Application and Threat Research Center. To learn how Milestone can help you fight back, call 866.646.9211 or e-mail info@milestonesystems.com.



Milestone Systems provides specialized network consulting services and web management/security solutions. The Milestone Review is designed to keep you informed about industry trends and ideas, as well as Milestone's products and services.

If you have any suggestions or comments, please e-mail us at newsletter@milestonesystems.com.

Milestone Systems
8401 Golden Valley Road,
Suite 300
Minneapolis, MN 55427 763-404-6236

Protecting Cardholder Data



Aberdeen Group's third annual study on PCI DSS shows that constant vigilance can help organizations achieve and sustain PCI compliance at 50 percent lower cost.

When you make an electronic transaction — either swiping a card at a checkout counter or through a commercial Web site — your payment information is sent to a payment card server run by the bank or merchant that sponsors the particular card. The server processes the payment data, communicates the transaction to the vendor and authorizes the purchase. Hackers are constantly looking for vulnerabilities that could allow them to take control of all or part of the server and potentially steal credit cards numbers and other information.

The Payment Card Industry (PCI) Data Security Standard (DSS), mandated by Visa, MasterCard and other card issuers, requires “all merchants with internal systems that store, process or transmit cardholder data” to comply with 12 key data protection measures and submit to security audits. Under the rules, companies must protect cardholder transaction data through logical and physical access controls, activity monitoring and logging, encryption and regular network scans. Companies could face penalties of up to \$500,000 for breaching customer credit card information.

In a new study on PCI DSS and Protecting Cardholder Data, the organizations earning top results were found to achieve and sustain compliance with PCI DSS at a 50 percent lower cost than all other respondents. The third annual study on protecting cardholder



Your behind-the-scenes IT team

When you need IT help, you can't afford to settle for anything less than great. The Milestone Advantage is built on a secure foundation of people, products and relationships. From engineers to project managers and sales professionals to trainers, the Milestone Systems team comprises the "best of the best."

In addition, Milestone Systems has hand-chosen business partnerships with select market leaders and innovators whose products and services represent the best solutions available in the marketplace today.

Contact us today to learn more!



866.646.9211
www.milestonesystems.com

data by Aberdeen Group, showed that consistent network vulnerability scanning, application vulnerability scanning, and penetration testing are core capabilities for enhancing security and achieving and sustaining PCI compliance.

The top-performing companies in the study are spending 61 percent less than all others in these areas, while achieving better results. The study found consistently large gaps between the leading and lagging performers in current use of technologies such as encryption, enterprise key management, content monitoring and filtering, and access management.

Milestone offers a number of solutions to help organizations meet PCI DSS requirements. For example:

1. F5 Networks' BIG-IP Application Security Manager (ASM) Firewall delivers comprehensive protection for Web applications. It can help your organization quickly pass a security audit without requiring changes to the application code. PCI compliance reports provide an executive summary of requirements and recommendations for bringing your application environment into compliance. F5's ASM employs unique technology that detects if your domains are being Web scraped of valuable information and shields your sites from copy and reuse.

2. PCI DSS requires that organizations assign unique IDs to employees with computer access and track them. Milestone Systems helps companies deploy SecureAuth 4.9.5 for VPN Authentication from Multifactor, which specifically addresses PCI compliance requirements for remote access to controlled systems. In conjunction with major VPN platforms, SecureAuth is able to deliver a secure credential, mapped directly to the individual user, utilizing the organization's existing data store.

3. For vulnerability scanning and penetration testing, Milestone recommends WhiteHat, a Web application testing software. "WhiteHat provides amazing visibility into your network!" explains Terry Shidla, CISSP at Milestone. A Web-based SaaS (Software-as-a-Service) Web site security solution, combining precision proprietary scanning technology with expert analysis, WhiteHat allows security professionals to easily find and fix Web site vulnerabilities before hackers can exploit them, and fulfill PCI testing requirements.

4. For the best-of-breed encryption, Milestone recommends Cisco-IronPort's Data Loss Prevention appliances to provide accurate and easy-to-use content-level filtering to detect sensitive data before it leaves the organization. If a sensitive message requires encryption, the message can be automatically encrypted using the Cisco IronPort Email Encryption feature – an agentless encryption mechanism that does not require PKI certificates, key management or any recipient training.

5. Milestone provides content monitoring via Check Point hard disk encryption. Check Point's Monitoring Software Blade shows a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events.

The threat landscape is constantly changing, and companies can neither adopt a "set and forget" approach to security nor hope that either the compliance requirements or the threats will simply go away. Most attacks can be avoided by being vigilant — regardless of whether the organization has been certified as PCI compliant.

To learn how Milestone can help enhance your network security, call 866.646.9211 or e-mail info@milestonesystems.com.

Phrying Phish



Tips to help keep your end-users from becoming victims of a fraudulent e-mail scam.

In October, the FBI announced a major cybercrime take down called Operation Phish Phry. The investigation uncovered a sophisticated international “phishing” operation that collected personal information from thousands of victims. The FBI says Operation Phish Phry is the largest cybercrime investigation to date in the U.S., with 53 defendants charged in U.S District Court.

According to the indictment, Egyptian-based hackers used phishing techniques to obtain bank account numbers and related personal identification information from bank customers. Phishing attacks frequently begin with an e-mail message purporting to be from a trusted source that actually contains a malicious link. The link directs users to a “spoofed” Web site that looks legitimate but is designed to trick users into disclosing personal information.

Unfortunately, nearly nine in 10 Web users in the U.S. are at risk of online fraud because they can’t identify the different forms of phishing currently happening online, according to a YouGov survey. Of the seven countries included in the research — the U.S., Germany, Sweden, Australia, India, Denmark and the U.K. — U.S. respondents were least likely to identify the signs of phishing.

The research asked respondents to identify which of two Web site images presented

side by side was a fraudulent phishing site. The most frequently missed telltale indicator was misspelling on the site, with 88 percent failing to spot the mistakes that often identify a phishing site. Other indicators that were missed by respondents included the lack of a padlock symbol in the browser address bar (68 percent), a URL containing an unspecified, numerical, domain name (42 percent) and unnecessary requests for additional account information (33 percent).

Fake Messages, Real Danger

Cybercriminals also use a number of other techniques to lure victims into clicking malicious links or opening attachments that carry malware. Fake messages that seem to signal a package pick-up from popular couriers are infected with Trojans. Fake receipts sent via e-mail are infected with malware that leave users vulnerable to identity theft. E-cards are another common source of phishing scams.

Cybercriminals use bogus discounts and promos to lure victims into clicking malicious links, or entering confidential information into fake sites. Typically, hot retail items are associated with such schemes are, making them irresistible to many users. In previous years, for instance, fake advertisements and Web sites for the Apple iPhone infected users with the Trojan TROJ_AYFONE.

Users who fill out seemingly harmless online surveys in exchange for gift cards, cash, free items or special promotions risk identity theft. Compromised survey pages are



MILESTONE TRAINING

Milestone Systems has a long history of providing relevant, quality training to our clients. We are an Authorized Training Center for F5 Networks and IronPort Systems in addition to offering classes in other technologies and certifications. We can customize a class to meet specific customer needs in numerous locations across the country. We can even come to your offices.

You can check out our upcoming courses or enroll online at www.milestonesystems.com/training/

milestone
systems, inc.



actually phishing sites designed to steal confidential information.

Cybercriminals also prey on users' generosity, using fake charity sites for a variety of scams. Typically, spammers send out messages pleading for donations to help victims of newsworthy calamities. Generous users who open the message and click on the link to donate end up robbed of cash and confidential information.

Social Networking Scams Surge

The FBI warns that there has been an increase in the hijacking of social networking accounts, citing a growing number of reports to the Internet Crime Complaint Center (IC3) about cybercriminals hijacking accounts and sending out distress messages claiming they are in some sort of legal or medical peril and requesting money from their social networking contacts. So far, nearly 3,200 cases of account hijackings have been reported to the IC3 since 2006.

Cybercriminals are also using spam to promote phishing sites, claiming a violation of the terms of service agreement or creating some other issue that needs to be resolved. Other spam entices users to download an application or view a video. Some of these messages appear to be sent from friends, giving the perception of legitimacy. Once the user responds to a phishing site, downloads an application, or clicks on a video link, the electronic device they're using becomes infected with malicious code.

According to industry researchers, the average loss from phishing is now over \$3,000 per incident and the total damages suffered by users victimized by phishing are well over \$1 billion per year. Banking and retail sites, including Amazon.com, Ebay and PayPal, have been

some of the most popular for criminals to impersonate with counterfeit sites using phishing schemes.

Social networking sites, such as MySpace and Facebook, are also key targets for "social phishing" since personal details included within such sites can be used in identity theft. Experiments show a success rate of over 70 percent for phishing attacks on social networks. Many phishers will try to get around anti-phishing solutions by using SSL encryption.

Blue Coat to the Rescue — in Real Time

The Blue Coat Real-Time Anti-Phishing protection technology assesses the Web page being requested using Blue Coat WebFilter and Dynamic Real Time Rating (DRTR). Blue Coat WebFilter runs on current ProxySG appliances and uses Dynamic Real Time Rating technology to keep up with the ever-changing Internet and phishing sites. DRTR is based on patented technology that can "on the fly" categorize new, unfamiliar Web sites as they are being requested and then block or allow a user's access according to the rating DRTR assigns and in accordance with the organization's or user's policies. The entire process can be completed in 250 to 750 milliseconds.

If the page is not found in the Blue Coat WebFilter database, a query is sent to Blue Coat Labs where the Web page is analyzed automatically in real time. Because these phishing Web sites are only up for a short time — ranging from hours to minutes — it's hard for most anti-phishing databases to catch them. This is why having a solution that assess URLs on the fly is essential.

Phishing is still a considerable threat. Newer tactics have lower visibility, lower risk, and high return rates. Fortunately most ploys can be thwarted through real-time assessment.