[UP LOAD]

By Stephen Trilling,
Senior Vice President

■▪ **SECURITY TECHNOLOGY AND RESPONSE**

Preventing Web-based Attacks

Symantec's intrusion prevention technology is increasingly valuable as malware authors shift their attack strategies

If you think the Internet is a safer place these days than 10 years ago, think again. Web-based attacks, where malware is installed on a user's system through a compromised Web browser or plug-in, are increasing in number and finding their way onto more legitimate websites. Many enterprises with otherwise robust endpoint and messaging security strategies are leaving themselves wide open to these threats.

The good news is that the technology to prevent these threats, an Intrusion Prevention System (IPS), is already included in Symantec Endpoint Protection—you just have to be sure it's turned on.

Anatomy of a drive-by download

Malware is no longer found only on malicious websites. Today, it is commonplace for legitimate mainstream websites to serve up malware to unsuspecting visitors. Due to the complexity of modern websites and the fact that content is often integrated from many providers, not all websites and advertisements are properly secured. In 2008, Symantec observed attacks from 808,000 unique domains, including popular news, travel, gaming, real estate, and even government websites.

Malware has traditionally been distributed through spam or through social engineering techniques that attempt to get a user to click and unknowingly download malicious code. However, hackers are now inserting malicious URLs into Web pages on legitimate websites, redirecting users to a malicious site that contains code designed to exploit specific vulnerabilities—with no user interaction required. This is often referred to as a "drive-by download," and attackers are increasingly turning to this method. Once malware is installed on the user's machine, the attacker can harvest personal information or take control of the machine to attack other computers.

Regular software patching helps, but even if your company installs the latest browser updates on all endpoints as soon as they are released, you may still be vulnerable. ActiveX controls, browser plug-ins, document readers, multimedia plug-ins, and other third-party applications often have vulnerabilities that are regularly exploited by malware authors.

An additional layer of protection

Because Web-based attacks are heavily obfuscated (disguised in the code) and dynamically changing, traditional signature-

MICHAEL MORGENSTERN

▮▪ SYMANTEC CHRONICLES

[Excellence in Service]
Symantec Enterprise Support Services was recognized at the Technology Services World Conference with a 2009 STAR Award for service excellence in mission-critical support. The award recognizes organizations for providing technical support in mission-critical environ-

ments where system uptime is imperative. STAR Awards, which began in 1990, are sponsored by the Technology Services Industry Association (TSIA). TSIA is the technology services industry's largest association, encompassing more than 50,000 members from 300 companies in 80 countries.

For more information, visit *go.symantec.com/star-award*.

[Green IT Delivers Results]
In a recent interview with *Enterprise Systems*, Symantec vice president of global solutions, José Iglesias explains how the company practices what it preaches in green computing.

Iglesias leads Symantec's efforts for sustainable computing, both internally and externally. "We have made a public commitment to reduce our carbon footprint 15 percent by 2012. Greening our IT infrastructure is a large part of how we will reach our goal and is part of our larger commitment to being a socially

Preventing Web-based Attacks

based antivirus solutions are no longer a complete solution. The attack must therefore be identified and intercepted before it even happens.

Symantec Endpoint Protection with Network Intrusion Prevention solves the problem by monitoring network traffic for suspicious behavior and stopping an attack before it threatens a user's system. "Vulnerability signatures" downloaded along with virus definitions are used to identify potential exploits. Generic Exploit Blocking technology uses these signatures to provide protection from vulnerabilities in the base operating system and Web browser, as well as vulnerabilities used by drive-by downloads—even if they aren't patched on the system.

Don't go on the Web without it
If protecting endpoints against the latest threats is important to your organization, don't allow your users to access the Internet without this essential layer of endpoint security. If you're already a Symantec Endpoint Protection customer, simply turn on Network Intrusion Prevention to enhance protection against Web-based attacks. If you're a Symantec AntiVirus customer who has not yet migrated to Symantec Endpoint Protection, you should upgrade to protect your organization against the primary vector of threats today. ■

>> A Delicate Balance
Integrating IT decisions into business strategy

Deloitte's 2009 IT-Business balance survey finds that IT is under tremendous pressure to deliver business value. The traditional "more automation at less cost" approach is passé. Now, IT is expected to show direct impact on dimensions such as customer satisfaction, better products, and growth in turnover and profit. But how, when one out of five responding companies says that IT strategy is rarely or never aligned with company strategy? About half rarely or never discuss IT matters at board level, and for the majority it is still a yearly exercise tied to the budget. There is hope, however: IT managers and their business counterparts confirm that the economic crisis has intensified fruitful dialogue between the two. To read the full report, visit *go.symantec. com/deloitte-balance*.

responsible company," Iglesias says. He notes that the company saved over $1.6 million in electricity costs for the calendar year 2008 by using its own software to drive IT operational efficiencies. With this, Symantec has already achieved 8 percent of the 15 percent target for carbon footprint reduction. For the complete interview, visit *go.symantec.com/ esj-interview*.

[Federal Law for Data Breach]
The U.S. Senate Judiciary Committee has approved two legislations that would require specified entities to safeguard personal information and notify individuals of any breaches. The Committee voted in favor of the Personal Data Privacy and Security Act of 2009 (S. 1490) and the Data Breach Notification Act (S. 139), sponsored

by Senators Patrick Leahy and Dianne Feinstein, respectively. In its current form, S. 1490 would require that covered entities, among other things, perform risk assessments, limit access to sensitive information, train their workforce, and require vendors by contract to implement appropriate safeguards. S. 139 would establish a national standard for federal agencies and businesses

engaged in interstate commerce to report data breaches. For more information, visit *go.symantec. com/privacy-report*.

[Seamless Integration]
The new, open remediation platform of Symantec Data Loss Prevention 10 will seamlessly integrate with leading solutions from GigaTrust, Liquid Machines, Oracle, and ···>

[UPLOAD]

>> The Gloom Lifts—Slowly

Asian Economies Lead the Swing in Sentiment

After reaching a nadir in January 2009, expectations for corporate profits and national economies turned sharply higher in June 2009, according to a McKinsey survey of 1,677 executives, representing all regions, industries, company sizes, and functional specialties. Since then, expectations have continued to rise in tandem with stock markets.
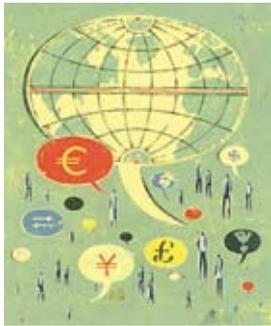
Nineteen percent of respondents around the world—and 28 percent in Asia's developed economies—say an economic upturn has already begun. However, there are striking differences in perceptions at the regional level. Executives in North America consistently indicate that the crisis will end sooner than executives elsewhere expect. Those in the Eurozone have consistently been gloomiest about their economic situation and outlook. A majority of the executives also don't expect GDP to rise soon, and 54 percent say that governments should scale back—but not stop—their support for economies.

For the complete report, visit *go.symantec.com/mckinsey-2009.*

>> Women Leaders Show the Way

What companies need during this time of crisis in corporate governance is the kind of leadership behavior most used by women—inspiring others and defining expectations and rewards. This was the feedback from 736 executives surveyed online by McKinsey in September 2009. Yet, the survey finds that far more corporate leaders are focusing on monitoring individual performance these days—even though this is seen as one of the least helpful ways of managing the crisis. The good news: a majority of the respondents say their companies have not cut back on programs to recruit, retain, and develop women. That said, only a third of the respondents consider gender diversity among their companies' top 10 priorities. For more on this, visit *go.symantec.com/mckinsey-leadership.*

Business Value Proof Points

IT Organizations Need Clear Markers for Valuing Investments

IT executives are all too familiar with the challenge of articulating the business case for new IT investments and, once deployed, presenting evidence of their impact. A series of new Business Value Analysis Market Research Reports (BVA-MRR), produced by The Alchemy Solutions Group, that draw on data gathered by Symantec worldwide surveys, offer insights.

Some of the hightlights include:
- For endpoint security, IT risk mitigation is the major driving factor for more than 60 percent of respondents during the next two years.
- As companies focus on dealing with the aftermath of security breaches, remediating intrusions is gaining mindshare—up 20 percent to 60 percent as a key decision-making factor in the next two years.
- Controlling growth of email storage and deduplication of data remains a priority for enterprise and large enterprises—focus will double over the next two years to 57 percent of respondents.

To view the three BVA-MRRs, visit the following:
go.symantec.com/bvamrr-endpoint
go.symantec.com/bvamrr-backup
go.symantec.com/bvamrr-archive

PGP Corporation. This will help companies better protect their data by applying encryption and enterprise rights management to sensitive content discovered through data loss prevention. It will also allow organizations to leverage existing investments in the PGP Encryption Platform, Oracle Information Rights Management, and Microsoft Active Directory Rights Management Services (RMS). For more information, visit *go.symantec.com/dlp10.*
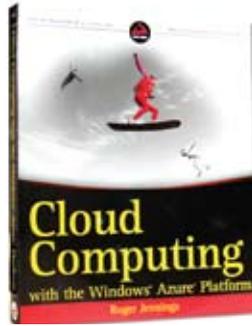
[Securing Patient Health Data] With the American Recovery and Reinvestment Act underway, healthcare organizations face new challenges to maintain privacy and security of patient health data. However, research indicates that many organizations may not be ready to meet the HITECH components of the ARRA legislation and other security challenges. This is the finding of the 2009 HIMSS Security Survey, sponsored by Symantec. The survey results show that security budgets remain low and organizations often don't have a response plan for threats or a security breach. Further, few have a designated CSO or CISO. Nearly 60 percent of respondents reported that their health organization spends three percent or less of its IT budget on information security. For more survey results, visit *go.symantec.com/himss-survey.*

Roger Jennings, *Cloud Computing with the Windows Azure Platform* (Hoboken, NJ: Wiley 2009)

ISBN: 978-0-470-50638-7
Price: $39.99

It's 1996, and Netscape owns the browser space with an 85 percent market share. Six years later, Navigator is present in trace amounts among users, and today it's gone for all practical purposes. Amazon is clearly king of the cloud computing hill. But Microsoft is on the brink of entering the cloud fray, and Azure has the potential to change the face of computing as we know it.

Roger Jennings' book, *Cloud Computing with the Windows Azure Platform*, introduces Azure from a technical point of view. Targeted first and foremost at developers, it puts cloud computing in historical context, describes the Azure platform, and dives quickly into roles and database tables and queues and how to write code that uses them. The book is filled with examples, both embedded and in the form of links to the author's website, as well as links to Microsoft and other sources.

Picking up Jennings' book from a bookstore shelf and leafing through it casually could be intimidating. There are pages of C#, http, and XML examples and dozens of screen shots. But it would be a mistake to dismiss it as a handbook for code jockeys. Wrapped around the programming details is a wealth of information that is as much, if not more, oriented toward managers and executives than toward programmers. The opening chapter's cloud ontology and advice to prospective adopters is a case in point. Sometimes it seems that "cloud" is whatever the person talking wants it to be. Jennings gives a concise description of "X as a Service" for a dozen or so values of X and presents some useful guidelines for approaching a cloud decision.

The bottom line on this book is that while it's aimed at developers (from whom it assumes quite extensive background knowledge), managers and executives who are wondering what the cloud will mean to them should have a look at it as well.

Paul Massiglia is a technical director in Symantec's Clustered Storage Products Group.

Peter A. High, *World Class IT: Why Businesses Succeed When Technology Triumphs* (San Francisco, CA: Jossey-Bass 2009)

ISBN: 978-0-4704-5018-5
Price: $38.00

It's about time. We now have a business book about IT. In *World Class IT: Why Businesses Succeed When Technology Triumphs,* author Peter High articulates the fact that IT is no longer just a corporate support function. In many cases, IT is the strategic element that drives a company's success.

What's unique about this book is that it's not only a must-read for the CIO (and everyone else in an IT department); it's for anyone associated with the technology industry. If you are a manufacturer, seller, or service provider of technology, you will gain insight into what makes an IT department world class.

There are three immediate takeaways in *World Class IT.* First, every IT employee should understand the overall mission, strategy, and goals of the company for which they work. Second, the best IT departments are populated with employees who understand the business they're in. Finally, if IT employees understand the first and second points, they will come away with a different view of what their true value and responsibility is to the company.

This is not just a book about IT theory. It provides a documented track with examples of successful companies that have followed what High describes as the Five Principles of World Class IT:

• Recruit, train, and retain world class IT employees
• Build and maintain a robust IT infrastructure
• Manage projects and portfolios effectively
• Ensure partnerships with the IT department and business
• Develop a collaborative relationship with external partners

World Class IT is truly a business book and not an IT book. CIOs who guide their departments to excellent performance in each of the five principles will be able to do so in other areas of their company as well. It is for that reason that today's world-class IT leaders will be tomorrow's successful CEOs.

Chuck Hegarty is vice president of Business Development & Alliances for ITS Partners.