INFORMATION SECURITY®

ESSENTIAL GUIDE TO

Threat Management

Attacks rise as the economy falls. Discover what technologies and policies can help you thwart them and protect your organization.

INSIDE

TechTarget
The Technology Media ROI Experts

INFOSECURITYMAG.COM

contents

ESSENTIAL GUIDE

THREAT MANAGEMENT

FEATURES

Business is Booming for Cybercriminals

BY KELLEY DAMORE

CYBER THIEVES DON'T get pink slips. In fact, business is booming for them in these troubled economic times. Just scan the headlines. Payment processor Heartland Payment Systems announced a breach that could trump TJX in size. Security vendors Kaspersky and F-Secure were hacked. Microsoft is offering a $250,000 reward for information leading to the arrest and conviction for those responsible for the fast spreading Conficker/Downadup worm which has yet to release its payload. And this all has happened in a 30-day time period.

So it comes as no surprise that threat management is a top priority for security pros despite tightened budgets and an uncertain future. Eight out of ten people expect to spend more or the same amount of time on threat management and web application security in 2009, according to the *Information Security*/SearchSecurity.com Priorities 2009 survey. What's more, as threats become more targeted and sophisticated, evolving threats remain a growing worry.

The *Information Security* Threat Management Essential Guide can help you decide what solutions are best for your organization and what you can do today to plug some of the holes in your security program.

In "Stretching Your Dollar," technical editor David Strom offers 10 tips that cost very little money and can help you lock down your networks. SearchSecurity.com and SANs instructor, John Strand, offers up predictions on the threat landscape for 2009 in "Enterprise Attacks in 2009."

Meanwhile, technical editor Joel Snyder explains the core differences between an IDS and an IPS in "Intrusion Detection or Prevention…or Both?" This article will help you figure out where you should make your investments. And as hackers are attacking the application layer, Michael Cobb explains what to look for when purchasing a Web application firewall in "Choosing the Right Web Application Firewall."

Lastly, *Information Security* Editor Michael Mimoso talks to a raft of security professionals to get their take on how to protect Web. 2.0 technologies, including Twitter, LinkedIn, Facebook and others.

We are in the midst of uncertain times and uncertain implications of new technologies. But one thing is certain, we'll arm you with the information you need to properly invest and improve your threat-management posture.›

Kelley Damore is Editorial Director of the Security Media Group for TechTarget, which includes Information Security *magazine, SearchSecurity.com, SearchMidmarketSecurity.com, SearchFinancialSecurity.com, SearchSecurityChannel.com, SearchSecurity.co.uk, Information Security Decisions conference and Financial Information Security Decisions conference. Send feedback on this column to feedback@infosecuritymag.com.*

STRETCHING YOUR DOLLAR

10 tips to protect your company in a recession.

BY DAVID STROM

TIMES ARE TOUGH for the good guys, but a recession is always an opportunity for criminals. Threats to your sensitive data, your customers and your infrastructure are increasing dramatically, from compromised and malicious Web sites to unhappy employees to poorly controlled partners.

The good news is that you can tighten your security and tighten your belt at the same time. Quick-payoff strategies can help you stay on top of evolving security threats without neglecting your network infrastructure.

There are many clever ways to do this. We'll look at 10 steps you can take to improve your threat management posture that require minimum investment, manpower and give you a fast return on your investment.

#1 Secure powered-down switches.

For a small effort, you can lock down unused network ports and at the same time save money by reducing your overall power consumption with switches (from Adtran and D-Link, for example) that turn off or power down when they're not needed. Your investment in this new equipment will pay for itself in a year or less.

Auto shut-off is a good way to secure your unused ports, by keeping prying PCs from entering your network at unexpected places and also helps physical security, especially in publicly accessible buildings such as hospitals and government offices.

#2 Check out lower-cost endpoint security.

There are dozens of endpoint security appliances and agents that come with hefty price tags and long implementation lead times.

If you want some of the benefits without the hassles and cost, then one solution is to purchase TPM-enabled laptops and start using some form of protection, such as fingerprint scanners or encryption keys that are stored on the TPM to keep unauthorized users away. The combination is a potent one since the TPM ensures that no one else can tamper with the scanned fingerprint to access the laptop.

Also, consider an appliances from Napera or eEye Digitial Security's Blink software. These are representative of a trend to lower-cost endpoint security products that are drop-and-replace solutions for Windows-only environments.

Napera looks like a network switch and works with a combination of agent-based software and firmware on the switch. You can enable protection on various ports and make sure that each PC that connects to these ports has updated anti-virus signatures and OS patches, and is malware-free before it connects to your network. It starts at $3,500 for a 24-port device, so this could be appealing for many small businesses. Or it could be deployed to protect public areas of your campus such as conference rooms and visitors' offices, where a lot of unknown laptops connecting to your network.

Blink offers a lot of protection for less than $30 a seat per year, including personal firewall, anti-virus and host intrusion prevention modules that are all part of its single agent.

#3 Get VPNs for free.

If you haven't implemented a VPN yet, now is the time to start. As your workforce becomes more mobile, there is more potential exposure to eavesdroppers at Wi-Fi hotspots and hotels. VPNs also come in handy when you want to extend a network share across the Internet securely, and have access to your files when you are on the road.

Certainly, you can spend tens of thousands of dollars on VPN technology.

But if you just want some basic and simple protection there are plenty of low or no-cost software alternatives that can do the trick, as long as you have a broadband connection at your disposal. One open-source offering is available at OpenVPN.org [http://openvpn.org/]; LogMeIn's Hamachi [https://secure.logmein.com/products/hamachi/vpn.asp] is another service that is free for personal use (a more robust version carries a low monthly fee) and easy to set up. There is also a listing at FileShareFreak [http://filesharefreak.com/2008/01/27/vpn-tunneling-for-private-p2p-connections/] with some other offerings, too.

The trick is making them universal for your staff to use, and providing support resources to guide the first-time VPN-ers through the process. The free VPNs could also serve as a stepping-stone to more capable products with heftier price tags and a way to justify their purchase later in the year.

#4 Avoid the Cisco "tax."

With the New Year, it is time to look at your annual support bills from Cisco, which you pay to keep current with IOS versions and for maintenance response time. I call this the "Cisco tax," and you should see if it makes sense to buy either a replacement device that you can keep as a spare or else find another vendor that doesn't charge for upgrades to their firmware/router operating system software. Again, this could be a very quick payoff, although it does involve spending some money to produce savings down the road.

#5 Deploy (almost) effortless encryption.

Certainly, encryption is one of those "nice to have, but hard to do" technologies that always seems to get on these lists. But, in recent years, a number of free or low-cost email and disk encryption tools have gotten better, so this could be the year to actually encrypt your removable disks and emails.

Two good places to start are the free open-source TrueCrypt [www.truecrypt.org] and Voltage Security's low-cost but easy-to-implement Voltage Security Network service.

TrueCrypt has a disk encryption client for Mac, Linux and Windows machines. Though it lacks enterprise management tools, it's excellent for small companies, executives and workgroups (for more on TrueCrypt [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1340488,00.html] check out Russ McRee's *Information Security* article). Voltage offers hosted email encryption that doesn't require any client installation and can work with Outlook and Webmail installations, all for about $65 per seat per year. Voltage handles all the administrative details, and the hosted service is quick and easy to implement.

And, of course, there is the long-time favorite from PGP, which is priced at less than $100 a seat, depending on what features you want to include. All of these products make managing the encryption keys extremely easy: one of

the drawbacks of implementing enterprise encryption is handling expiring keys when employees leave, or recovering them when they forget their key.

You could also turn on BitLocker and FileVault in the native Windows and Mac OS, respectively. They provide extra protection without spending an extra dime. However, they are hard to deploy across the enterprise—you definitely get what you pay for here.

#6 Get to know your IDS.

You might think simply having an intrusion detection system is enough of an achievement, but it is time to get up close and personal with your IDS and do a better job of tuning it to your particular circumstances. This means adjusting its configuration, understanding its reports and logged activities, and doing some rudimentary analysis.

You might think simply having an intrusion detection system is enough of an achievement, but it is time to get up close and personal with your IDS and do a better job of tuning it to your particular circumstances.

Granted, there is never enough time in the day, but if you are going to stay on top of the latest threats, you need to spend some more time with your IDS analysis to understand what it is telling you. If you are using Snort as your main IDS, check out Richard Bejtlich's podcast [http://media.techtarget.com/audioCast/SECURITY/richard_bejtlich_snort_FAQ.mp3] and check out forums on snort.org [http://www.snort.org] to gain more expertise.

Another option is to send one or two of your staff to get additional training in understanding your system's features and ways that you can tighten it up. While training budgets are the first to go in a recession, this is one investment that can provide quick paybacks, and provide additional threat protection with very little incremental effort.

#7 REALLY terminate ex-employees.

We're talking about the waves of layoffs of all types of employees, not just in the IT department. As your company contracts, the biggest threats are from staff who have been on the inside and are now jobless. Studies have shown that an ex-employee can be a security nightmare. Never changed any of your passwords on key servers? Do you have the same master password for multiple machines? Now is the time to change that behavior.

You should also do an assessment of other risks from newly terminated staff. Are your access control policies up to date? Did you disable all the security keys, passwords and access codes? Do you know if your remote gateways

are still be used by these people? Time to check access logs and make sure that the access directory entries of the departed are removed as well.

#8 Get Rid of SQL injection once and for all.

It is amazing that an exploit so long in the tooth can continue to affect, even destroy, so many servers. SQL injection is basically a back door entry into your databases through unprotected Web pages. A hacker can create and execute it without any programming knowledge and little skill. Why is this still a source of pain?

One reason is that really eliminating SQL injection requires the cooperation of several different departments, working together to make sure that the vulnerabilities aren't ignored. Another reason is that vulnerable sites are easy to find, especially since a couple of quick Google searches with a few keywords can often uncover problems without a hacker having to even enter your network with any probes. (Check out this good quick tutorial on protecting yourself from Google hacking [http://www.informit.com/articles/article.aspx?p=170880&seqNum=4].)

It is amazing that an exploit so long in the tooth can continue to affect, even destroy, so many servers

So, let's try to stamp this out forever this year; take the time to really go through your applications to make sure that it doesn't find you on someone's list next fall. Do an audit, hire a specialist consulting firm, or get educated on how to fix your database/Web server programming to prevent what is still an unfortunately common exploit from happening. Go to OWASP.org [http://www.OWASP.org] and get lots of tips on how to set up your database access properly and understand exactly why and how you are vulnerable.

If you want something more potent, you can download a free version of Acunetix's Web Vulnerability Scanner and various free trials of HP's assessment tools [https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5E14344_4000_100__], such as WebInspect.

Another thing to try is modsecurity.org's [http://www.modsecurity.org] open-source Web App Firewall; check out this *Information Security* article on modsecurity [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257087,00.html] to learn how to get the most from this tool.

Of course, just because you downloaded the free scanner and didn't find anything at first doesn't mean that you are protected for all eternity, but at least you can get a start on how to use these tools and understand how you are vulnerable. The trick is doing a regular series of scans to make sure that no one created any new backdoors.

#9 Stop data leaks.

One data breach lawsuit can ruin your whole day. As more data traverses the Internet, it makes sense to look at lower-cost tools that can stop data leaks or at least be more proactive about them. Code Green Networks and eTelemetry Metron SE are examples of monitoring products that can be easily deployed and don't cost as much as some of the alternatives. They can also scale up to some fairly large installations.

Granted, this is spending probably more dough than you want to—we are talking five- or six-figure purchases here—but, still, if you have tried some of the other lower-cost steps we recommend this might be a smart place to make a moderate investment.

#10 Pay your own people to find innovative solutions.

This is so simple and easy to implement that you will wonder why you didn't think of it. Set up a reward system to foster out-of-the-box thinking and ways to tune your security posture by having your own staff make and then benefit from their suggestions. You can avoid hiring consultants and increase morale at the same time. Your own people are the real experts when it comes to understanding the major weaknesses of your systems. The more you can encourage them to come forth, the better for everyone around. ›

David Strom is an expert on Internet and networking technologies who was the former editor-in-chief at Network Computing*, Tom's Hardware.com, and DigitalLanding.com. He currently writes regularly for PC World, Baseline Magazine, and the New York Times and is also a professional speaker, podcaster and blogs at strominator.com and WebInformant.tv. Send comments on this article to feedback@infosecuritymag.com.*

TRENDS

Enterprise Attacks in 2009

BY JOHN STRAND

The past may be a prologue to the future, but familiar threats–wireless, operating systems and others–will take on a new insidiousness in 2009.

WIRELESS RISKS CONTINUE

There are so many ways to attack a client system via wireless vulnerabilities, as you can see just by looking at Karma, a set of tools for assessing the security of wireless clients, and karmetasploit, a tool that acts as a wireless access point and responds to all probe requests from wireless clients.

Many organizations are about five years behind the curve when grappling with Wi-Fi threat vectors. The concept of wire-side attacks is becoming well known in many management circles, but it has taken some time. While wireless has been around for a while, the core of many wireless security policies is simply to not use the inherently insecure WEP protocol. Unfortunately, there needs to be a greater focus on other vulnerable protocols and the variety of other wireless attacks. Traditionally we have viewed our risks in terms of a network perimeter. As we extend our networks with wireless connectivity, vendors implement new protocols and authentication schemes like TKIP, LEAP and PEAP in different ways. We need to fully research the protocols used by our vendors before implementing them in our organizations.

RETURN OF OPERATING SYSTEM ATTACKS

While operating system attacks have not reached the effectiveness and prominence they had from 2003-2005, malicious hackers will most likely discover operating system vulnerabilities again. There has been a tremendous amount of research over the past few years in browser-based attacks like cross-site scripting (XSS), cross-site request forgery (XSRF) and clickjacking. But what if these techniques were used in conjunction with an operating system vulnerability?

We will begin to see more hybrid threats that target weaknesses in Web servers and browsers while also damaging the OS. If attackers can compromise one machine, they can utilize OS attacks against additional internal systems, allowing malicious hackers to greatly extend the damage of their tactics. Because of this convergence, we'll need to start identifying possible security blind spots, like the applications installed on our desktops. We'll also need to develop mechanisms to identify vulnerabilities in applications beyond our servers and operating systems.

MORE STRAIN ON ANTIVIRUS PRODUCTS

The release of Metasploit 3.2 is a watershed event. With the security exploit platform's capability to dynamically encode malicious payloads, it's now possible for novice attackers to bypass an enterprise's antivirus software. Using a few simple commands, a hacker can generate a piece of malicious software that will bypass most (if not all) of the current signature-based antivirus products.

This trend has been a long time in the making; however, 2009 will bring attacks using these techniques in targeted situations. Employing Metasploit to create part of a worm or a botnet will provide limited utility, as the AV vendors will be quick to release

EDITOR'S DESK

TABLE OF CONTENTS

STRETCHING YOUR DOLLAR

INTRUSION DETECTION OR PREVENTION?

CHOOSING A WEB APPLICATION FIREWALL

HOW TO SECURE WEB 2.0 TECHNOLOGY

a new signature. However, if one organization is targeted for a specific goal—think Department of Defense, credit card companies or organizations possessing health information—the damage can be inflicted quickly. Without the need for a long-term, persistent attack, a hacker can use Metasploit to get in, get what he or she wants and get out.

As an alternative, many organizations should look into security products that also include application heuristics, which flag malware based on recognition of improper behavior rather than a signature, as well as application whitelisting techniques.

MORE LIMITATION ON USERS' WEB SURFING

When many organizations look at their main vectors of compromise, one thing is going to stand out above all others: corporate user Web surfing. Why exactly do many companies allow their users to surf the Internet? Some organizations need their users to be able to do research, but many enterprises allow this activity because they want their environment to be a "fun place to work." At some point, every company needs to weigh the benefits of letting their users surf the net versus the risk of attack through that vector.

Almost all of the compromises I help my customers with today are the result of an internal user surfing to a site that is hosting malware. Currently, this is the easiest way for attackers to bypass all of the shiny IDS/IPS/NAC/AV technology that organizations implement.

Even if your organization needs to allow a certain portion of their users to access the Internet, stronger approaches exist that can be utilized. For example, you could isolate those systems from the rest of your network via a segmented VLAN.

TRAINING BUDGET BATHTUB

Training budgets are going to get cut in 2009. There is no question about that. However many organizations are going to reduce security resources as more of a kneejerk reaction to overall reductions in revenue and budgets. Information security is not something that is stagnant. The threats are constantly evolving, and an organization's security staff must evolve with it. By cutting their security training budgets, some organizations will fall behind. We are going to see an upswing in training budgets for security in the second half of the year as organizations begin to realize the seriousness of emerging threats. Because of the dynamic nature of our profession, there is a constant need for training to stay current on the newest attack vectors and, more importantly, defenses.

FEWER VENDORS SAYING "HACK PROOF"

Finally, this is just a small request. Lately an increasing number of vendors using this phrase again. I have some simple advice for vendors who are planning on using this phrase to market their products: don't do it. You're only daring malicious hackers to try to compromise your product, and with enough time and effort, ultimately anything can be compromised. This is why a defense-in-depth approach that does not rely on any one product or method is so critical for enterprises. To that end, enterprises should always be wary of any product marketing slogans that seem too good to be true, because they probably are.

John Strand currently is a Senior Security Researcher with his company Black Hills Information Security, and a consultant with Argotek, Inc for TS/SCI programs. He teaches the SANS 504 "Hacker Techniques, Exploits and Incident Handling," 517, "Cutting Edge Hacking Techniques," and 560 "Network Penetration Testing" classes as a Certified SANS Instructor. Strand also answers your questions on information security threats.

Intrusion detection or prevention?

Which way should you turn?

We'll cut through the hype and explain the benefit of both technologies

BY JOEL SNYDER

WHILE THREAT MANAGEMENT continues to be a top priority, it is more important than ever for cash-strapped security professionals to fully understand the functionality of intrusion defense tools in order to make good purchasing decisions.

Intrusion defense systems (IDS) and intrusion prevention systems (IPS) are a particularly confusing area because the products are so similar, the vendors are all the same, and even the acronyms are hard to tell apart. We'll explain the capabilities of each and how to decide whether you need one or both technologies.

Differentiating IDS and IPS

An IPS is not the same as an IDS. However, the technology that you use to detect security problems in an IDS is very similar to the technology that you use to prevent security problems in an IPS.

It's important to start out with the understanding that IDS and IPS are very, very different tools. Even though they have a common base, they fit into the network in different places, have different functions, and solve different problems.

An IPS is best compared to a firewall. In a typical enterprise firewall, you'll have some number of rules—maybe a hundred, maybe a thousand. Most of those rules are "pass" rules: "allow the traffic through." Thus, the firewall gets a packet off the wire and starts through its rules, looking for a rule that says "allow this packet through." If it gets to the end of the list and there's no rule saying "allow this packet through," then there's a final "deny" rule: "drop everything else." Thus, in the absence of a reason to pass the traffic the firewall drops it.

And IPS is like that, but inside out: it has rules, maybe hundreds, maybe thousands. Most of those rules are "deny" rules: "block this known security problem." When a packet shows up at the IPS, the IPS looks through its rule list from top to bottom, looking for some reason to drop the packet. At the end of the list, though, is an implicit "pass" rule: "allow this packet through." Thus, in the absence of a reason to drop the traffic, the IPS passes it through.

Firewalls and IPSes are control devices. They sit inline between two networks and control the traffic going through them. This means that the IPS is in the policy side of your security house. It's going to implement or enforce a particular policy on what traffic is not allowed through.

The obvious affinity of firewalls and IPSes from a topological point of view has led us to the world of UTM, where an IPS is incorporated into the firewall. UTMs let you have both security services (blocking security threats, and allowing known good traffic) into a single device. *(For more, see p. 19)*.

The main reason to have an IPS is to block known attacks across a network. When there is a time window between when an exploit is announced and you have the time or opportunity to patch your systems, an IPS is an excellent way to quickly block known attacks, especially those using a common or well-known exploit tool.

The main reason to have an IPS is to block known attacks across a network.

Of course, IPSes can provide other services. As product vendors search to differentiate themselves, IPSes have become rate limiting tools (which is also helpful in Denial of Service mitigation), policy enforcement tools, data leak protection tools, and behavior anomaly detection tools. In every case, though, the key function of the IPS is a control function.

What do IDSes do?

If an IPS is a control tool, then an IDS is a visibility tool. Intrusion Detection Systems sit off to the side of the network, monitoring traffic at many different points, and providing visibility into the security posture of the network. A good analogy is to compare an IDS with a protocol analyzer. A protocol analyzer is a tool that a network engineer uses to look deep into the network and see what is happening, in sometimes excruciating detail. An IDS is a "protocol

analyzer" for the security engineer. The IDS looks deep into the network and sees what is happening from the security point of view.

In the hands of a security analyst, the IDS becomes a window into the network. The information provided by the IDS will help the security and network management teams uncover, as a start:

- Security policy violations, such as systems or users who are running applications against policy
- Infections, such as viruses or Trojan horses that have partial or full control of internal systems, using them to spread infection and attack other systems
- Information leakage, such as running spyware and key loggers, as well as accidental information leakage by valid users
- Configuration errors, such as applications or systems with incorrect security settings or performance-killing network misconfiguration, as well as misconfigured firewalls where the rule set does not match policy
- Unauthorized clients and servers including network-threatening server applications such as DHCP or DNS service, along with unauthorized applications such as network scanning tools or unsecured remote desktop.

This increased visibility into the security posture of the network is what characterizes an IDS, and which differentiates the visibility function of an IDS from the control function of an IPS.

Of course, since both IDS and IPS have the word "intrusion" as the beginning of their acronym, you may be wondering why I haven't mentioned "intrusion" as part of the function of either IDS or IPS. Partly that's because the word "intrusion" is so vague that it's difficult to know what an intrusion is. Certainly, someone actively trying to break into a network is an intruder. But is a virus-infected PC an "intrusion?" Is someone performing network reconnaissance an intruder…or merely someone doing research? And if a malicious actor is in the network legitimately—for example, a rogue employee—are their legitimate and illegitimate actions intrusions or something else?

The more important reason for leaving "intrusion" out of the description for both IDS and IPS is that they aren't very good at catching true intruders.

The more important reason for leaving "intrusion" out of the description for both IDS and IPS is that they aren't very good at catching true intruders. An IPS will block known attacks very well, but most of those attacks are either network reconnaissance or automated scans, looking or other systems to infect—hardly "intrusions" in the classic sense of the word. The best Intrusion Prevention System in this case is the firewall, which doesn't let inappropriate traffic into the network in the first place.

It's the misuse of the word "intrusion" in referring to these visibility and control technologies which has caused such confusion and misguided expectations in staff at enterprises that have deployed either IDS or IPS.

Yes, an IDS will detect true intrusions. Yes, an IPS will block true intrusions. But these products do much more than that—they provide greater control and greater visibility, which is where their real value is.

So which do I buy?

If all products were either an IDS or an IPS, then the answer to the question of "which should I buy" would be easy: buy an IDS if you want visibility, and buy an IPS if you want control. But IPS and IDS vendors don't make it easy for us, because they have developed and released hybrid products which combine IDS visibility on top of IPS control.

For most enterprises, especially ones who don't have an IPS or an IDS already, the right answer is "buy an IPS." A visibility tool only brings you value if you have time to look at what it's telling you. With tight budgets and overstressed staff, the kind of senior security engineer it takes to really get value out of an IDS is in short supply. Buying a product that no one is going to look at isn't going to do you much good. Without regular and disciplined use of the visibility aspects of an IDS, the only real effect you'll see is in increased power bills.

This doesn't mean that an IPS is a "set it and forget it" kind of device. To get value out of an IPS, you must tune it to match your own network and application and system mix. If you don't, you'll either have a high rate of false positives, which can interrupt legitimate traffic, or you'll miss a lot of attacks, in which case the IPS is not bringing you very much value. An IPS that never has a false positive is probably not doing a good job at protecting your network.

However, you will get value out of an IPS without a large time investment in managing and tuning it, and analyzing what it's telling you about your network. That's because the IPS will be there, providing additional defenses, and helping to protect you against common

ALL-IN-ONE

What about UTM IPSes?

THE COMBINATION OF an IPS and a firewall into a single system, with a single management system, is attractive. Unfortunately, most unified threat management systems (UTMs) are designed for SMB deployment, an environment where the simplicity of the management system is one of the most critical design requirements. Combining IPS management with firewall management is a very difficult task. In fact, no product vendor has successfully managed to merge their Web-based firewall management system with a good IPS management tool.

You shouldn't assume that an IPS incorporated into a UTM firewall will offer the same types of controls and protections as a standalone IPS.

This does not mean that there aren't great UTM firewalls with embedded IPSes; it just means that the management systems for the IPS part of these products are quite different (and often separate) from the firewall parts.

If your prospective UTM firewall vendor has bundled the IPS and firewall functionality all into a homogeneous single Web interface, you're looking at a product where the IPS is getting second rate management tools. This may be fine in environments where you're only interested in control, such as at branch offices or where only a small set of systems are being protected.

To find an enterprise-class IPS combined with a UTM firewall, look for products which are, paradoxically, less integrated: a standalone IPS and standalone firewall combined in the same chassis, for example.

–JOEL SNYDER

EDITOR'S DESK

TABLE OF CONTENTS

STRETCHING YOUR DOLLAR

INTRUSION DETECTION OR PREVENTION?

CHOOSING A WEB APPLICATION FIREWALL

HOW TO SECURE WEB 2.0 TECHNOLOGY

errors. Since most security problems are the result of human error rather than targeted attacks, the IPS is an outstanding way to bring a defense-in-depth strategy to network security.

Most IPS vendors, because of their IDS heritage, sell products which actually combine both IPS and IDS functions. They have the powerful malware and attack recognition engine needed to identify and block attacks, but they also have additional rules and tools designed to enhance network visibility.

As you're considering IPS, IDS, or combination products, remember to focus on your primary requirement. If you are looking for additional control, the most important part of the picture is the IPS detection engine. IPSes need the ability to quickly detect and block attacks, at very high speeds and without degrading network performance, throughput, or latency.

If you're looking for visibility, network forensics, and analysis capabilities, the most important part of the picture is the IDS management console. You have to be able to navigate through the information provided by the IDS in a quick and natural way to gain network and security visibility. While the detection engine is important, it's not nearly as important as the management system. Without an effective way of extracting information from the IDS—and this is as much your training as it is the management console you install—you won't see much value from an IDS.

Joel Snyder is Senior Partner for Opus One. Snyder has built and secured some of the largest and highest profile networks in the world for major ISPs, government agencies and Global 2000 companies for the past 27 years. In addition to many consulting projects, Joel has authored several books and hundreds of technical articles; designed compilers, data management applications, conferencing systems, security systems, and anti-spam tools. Snyder is also a technical editor for Information Security *magazine and has written numerous feature articles and technical reviews on subjects including e-mail security, spam controls and security management systems. Send comments on this article to feedback@infosecuritymag.com.*

CHOOSING THE Right Web Application Firewall

The application layer is the newest threat vector. We'll show you how to pick the WAF that's right for you.

BY MICHAEL COBB

BY USING APPLICATION-LAYER ATTACKS, cyber criminals can gain administrative or root privileges to execute malicious commands, install Trojans or backdoors or hijack accounts to get passwords or confidential information.

According to an *Information Security*/SearchSecurity.com Priorities 2009 survey, 38% of the 900 respondents planned to spend more time on application security in 2009 and 20 percent said it was a major security problem for them.

One of the solutions to prevent against such an attack is a Web application firewall or application-layer firewall. A WAF can be an appliance or software designed to protect Web applications against attacks and data leakage. It sits between a Web client and a Web server, analyzing application layer messages for violations in the programmed security policy. Web application firewalls address different security issues than network firewalls and intrusion detection/prevention systems, which are designed to defend the perimeter of a network.

What you need to know

First to choose a security device such as a Web application firewall (WAF), you need to answer the following questions:

- What does it need to do based on your security policy objectives and legislative requirements?
- What additional services would be valuable?
- How will it fit into your existing network—do you have the in-house skills to use it correctly and effectively?
- How will it affect existing services and users and at what cost?

A good security policy defines your objectives and requirements for securing your data. That foundation allows you to define what security devices are appropriate to meet your requirements. Since each Web application is unique, security must be custom-tailored to protect against the potential threats identified during the threat modeling phase of your secure lifecycle development program. Review which of these threats the WAFs under consideration safeguard against—such as analyzing parameters passed via cookies or URLs and providing defenses against all of the OWASP Top Ten application vulnerabilities—as well as any additional requirements mandated for compliance.

A good security policy defines your objectives and requirements for securing your data.

Choosing your WAF

In general WAFs must be able to inspect and handle Web page content such as HTML), Dynamic HTML (DHTML), and cascading style sheets (CSS), as well as the protocols that your application uses, such as HTTP and HTTPS.

Also, check how quickly the vendor has adopted new protocols in the past. Review their development and support policy to determine if they will support custom protocols or protect a set range of application protocols. In addition, a WAF must be able to inspect Web services messages, typically SOAP and XML. Ask the WAF vendor about their processes for auto-updating and applying dynamic signatures. Such conversations will help you assess their technical support and help services.

Lastly, ask about the additional cost of specific features. For example, some applications may require FIPS hardware key store support. A WAF vendor may support this requirement but at a dramatically higher price.

As you work through the list of requirements, take the time to understand the technical approaches and depth of treatment that each WAF uses to provide coverage of one or more security areas. Can you whitelist data types and ranges and create rules combining both white and black lists? How strong is the WAF against attack on itself? For example, it should run on a hardened OS, probably with components running in a non-privileged and closed runtime environment. If the product's security isn't rock solid, you should probably end the discussion right there.

Software versus hardware

A WAF can be implemented in software on a standard server running a common operating system or an appliance. It may be a stand-alone device or integrated into other network components. So, you can choose from the full range of WAFs on the market.

Software WAFs are usually cheaper and more flexible. Appliances are typically easier to install and configure, partly because their operating system has already been hardened, whereas a software firewall will require you to harden it. (A WAF won't protect you against poor configurations or vulnerabilities in your servers.)

If you opt for a software-based product, choose one that works on a platform with which your IT department is familiar. Either way, check out what type of training and support is provided by the firewall vendor—and at what cost.

There are, of course, open source software WAFs, such as ModSecurity[http://modsecurity.org] and AQTRONIX WebKnight [http://www.aqtronix.com]. If they meet your requirements you can greatly reduce your costs, but you will still need staff to learn, install, configure, and maintain it. Many open source projects have excellent support forums but unlike a purchased product you won't be able to call a help desk in an emergency.

Performance and scalability are other important considerations when evaluating hardware or software options. Some devices may be limited as to how many transactions per hour it can handle. Other appliances may have bandwidth limitations. You will need to choose a scalable and flexible firewall if you're planning on increased Web activity or adding applications in the near future.

Software products often provide an easier upgrade path than appliances, but hardware WAFs are better suited for high-volume sites, which require high throughput.

If you are running a large-scale application, which requires more than one WAF, then centralized management may be a critical feature so firewall policies can be deployed and managed from a single location.

Our advice is not to get hung up on whether the WAF is hardware or software, as long as it can meets your objectives and you have the in-house skills to configure and manage it.

Help is on hand

Plan on devoting plenty of time to fully evaluate WAF products. Once you have narrowed down your choices to those that meet your basic requirementhow do you compare the different options?

BY THE NUMBERS

Choosing a Web Application Firewall

FOLLOW THESE BASIC STEPS IN SELECTING THE APPROPRIATE WAF FOR YOU APPLICATION:

1. Use security policy objectives to define what controls your WAF must have.
2. Review the types of risk each product covers.
3. Test performance and scalability.
4. Evaluate the vendor's technical support.
5. Assess whether you have the required in-house skills to maintain and manage it.
6. Balance security, throughput, and overall cost.

The Web Application Security Consortium (WASC) [http://www.webappsec.org/] creates and advocates standards for Web application security. They have developed the Web Application Firewall Evaluation Criteria (WAFEC) [http://www.webappsec.org/projects/wafec/] for comparisons. Their testing methodology can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.

These tests should be part of your evaluation process. Follow WASC's recommendation to pay close attention to the deployment architecture used, support for HTTP, HTML and XML, detection and protection techniques employed, logging and reporting capabilities, and management and performance.

WAF deployment

Congratulations, you've chosen, purchased and installed a WAF. Installation needs to follow the four-step security lifecycle: Secure, monitor, test and improve. This is a continuous process that loops back on itself in a persistent cycle of protection. Before any device is connected to your network, you need to ensure that you have documented the network infrastructure and hardened the device or the box it will run on. This means applying patches as well as taking the time to configure the device for increased security.

Careful testing is essential, particularly if your site makes use of unusual headers, URLs or cookies, or specific content that does not conform to Web standards.

Configuration will stem directly from the business rules that you've established in your security policy (such as allowed character sets). If you approach firewall configuration this way, the rules and filters will define themselves. WAFs can expose technical problems within a network or application, such as false positive alerts or traffic bottlenecks.

Careful testing is essential, particularly if your site makes use of unusual headers, URLs or cookies, or specific content that does not conform to Web standards. Extra testing time should be allowed if you are running multi-language versions of your application, as it may have to handle different character sets.

The testing should match the "live" application environment as closely as possible. This will help expose any system integration issues the WAF may cause prior to deployment. Stress testing the WAF using tools with Microsoft's Web Application Stress and Capacity Analysis Tools or AppPerfect Load Tester will also help reveal any bottlenecks caused by the positioning of the WAF.

WAF management

Once you're up and running, assess how any future Web application firewall changes may impact your Web applications, and vice versa. You must, of course, document the changes you make to your network infrastructure for future reference and troubleshooting. This involves tracking any changes made to their configuration now and in the future.

Changes to the production environment should always occur during a monitored maintenance window. Make sure all affected parties throughout the organization are

advised in advance of the timing and scope of the changes. To ensure that configurations aren't changed unintentionally or without due process, you must control physical as well as logical access to your security devices. Strict adherence to change control, business continuity, and disaster recovery policies will all play a part in protecting the WAF and your business.

Because application-layer firewalls examine the entire network packet rather than just the network addresses and ports, they have more extensive logging capabilities and can record application-specific commands. So, don't let this capability and information go to waste. Log file analysis can warn you of impending or current attacks. Ensure that you define what information you want your firewall to log—preferably the full request and response data, including headers and body payloads. Make sure your staff has the expertise—and adequate time—to review and analyze it.

Web applications will never be 100 percent secure. Even without internal pressures to deploy Web applications quickly, there will be vulnerabilities that are open to threats. By having a Web application firewall in place as part of a layered security model, you can observe, monitor and look for signs of intrusion. It can also mean the difference between scrambling to fix a vulnerability or having the breathing room to repair the vulnerability to your own timetable.

Michael Cobb, CISSP-ISSAP, is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. Cobb is the guest instructor for SearchSecurity.com's Messaging Security School and, as a SearchSecurity.com site expert, answers user questions on application security and platform security. Send comments on this article to feedback@infosecuritymag.com

What's Next?

Web application firewalls are just the start.

TO COMBAT THE ever increasing sophistication of application attacks, the protection offered by WAFs should be integrated into application assurance platforms. This structure, promoted by vendors such as F5 and Barracuda, combines WAFs, database security, XML security gateways and application traffic management to provide more holistic security coverage.

The benefits include the ability to compare information across these devices to accurately determine if traffic is potentially malicious. This makes traffic control, analysis and reporting far more effective. Administrators can configure one set of policy rules and parameters, rather than trying to enforce each policy across several different devices,greatly reducing administrative overhead.

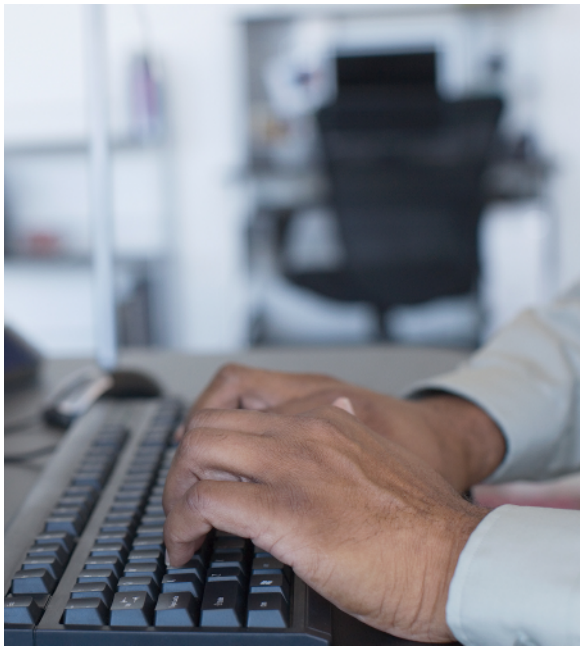
Looking into the future, it is essential that WAFs or whatever supercedes them gain the ability to interpret inbound data the same way as the application it is protecting. This will entail some form of script engine to remove any obfuscation, so that the security device will view the request in the same form that the browser will. This will make it far easier to assess whether or not the code is malicious. Let's hope we will see this form of dynamic analysis in the next generation of security devices. ›

–MICHAEL COBB

HOW TO SECURE WEB 2.0 TECHNOLOGY

Experts advise to be judicious when it comes to adoption and usage.

BY MICHAEL S. MIMOSO



ADMIT IT: YOU HAVE A LINKEDIN PROFILE, perhaps even Facebook page and a Twitter account. Personally it allows you to remain connected to current and former colleagues, friends and family. But as a security professional, these same social networking sites are cause for alarm because of the malware and data leakage concerns.

The problem is today's primary means of small talk can be a risk to sensitive corporate and private information. People who Twitter in their personal lives, for example, also tend to bring those 140-character Tweets into their professional lives, and the line can become blurred as to how much information becomes too much information.

Paranoia? Not really.

Take LinkedIn: it's a haven for mining competitive intelligence. Threats expert Lenny Zeltser wrote recently for the SANS Internet Storm Center that attackers are checking out company profiles for title changes that would indicate strategy or organizational shifts. New hires show up on company profiles, too; they're fresh meat for attackers because newbies aren't up to speed on company policy or security culture. Sophisticated attackers can also map organizations via these profiles in order to target attacks.

Web 2.0 has radically messed with the way information and even marketing material is disseminated and consumed. Twits (the affectionate nickname for folks on Twitter) scooped CNN.com on the January crash of USAir flight 1549 into the Hudson River. Blogs, RSS feeds and Craigslist have pushed newspapers and their day-old analysis of news to the brink of extinction. Many companies are building their brands via social networking, going as far as disseminating press releases and product announcements via Web 2.0.

It's an immediacy not even email can offer. But like any business implement, there must be controls and finding a happy security balance between policy and technology is tricky. Banning social networking—and by extension, Web 2.0—in the enterprise is akin, as expert Marcus Ranum likes to say, to complaining after a horse has left an unlocked barn. The next-generation workforce has Web 2.0 neatly packed away in their backpacks and intends to use it at their desks; it's up to the security industry to work with business management to contain the threat of its side effects: information leakage, malware infestations and productivity drain.

SERIOUS RISKS: MALWARE, DATA LEAKAGE

User generated content is what separates today's Web 2.0 from yesterday's online experience. People love to share the most innocuous things with their online friends, download silly applications and manage what they believe to be their private space on the Internet. The companion truth is that attackers have followed their prey to social networking platforms, and are laying down phishing snares, infecting machines with ad-generating software and logging keystrokes.

In the business world, the dangers to corporate secrets are growing. As business embraces these new mediums, the odds grow that someone could inadvertently spill secrets on a blog or collaboration portal, or follow links in a Facebook app to a phishing or malware site and either lose personal information or afford an attacker unfettered access to a corporate network.

User generated content is what separates today's Web 2.0 from yesterday's online experience.

"In the old days, you put up content on a website and people can browse it. Hopefully, the website is under the control of one party and it's easier to inspect content and make sure it's legitimate," says Chenxi Wang, principal analyst at Forrester Research. "Now with social networking, you're involving a large number of parties who are all uploading content; it's very difficult to attain the same level of assurance."

Wang says companies are getting less Draconian about social networking use inside the firewall. If there is a business purpose, it is allowed, even if it is restricted somewhat; it's also a useful in helping attracting younger workers. She points out that in some heavily regulated industries, such as financial services and health care where communication must be logged, policies are stricter on content that leaves over the Web. Webmail, i.e., Gmail and Yahoo, is a concern there, as are peer-to-peer file sharing resources and online storage containers such as Megaupload; knowledge workers could use these resources to circumvent policies on what types and how documents are allowed to leave the network.

"I think companies need to be judicious about Web 2.0 adoption and usage; don't use anything the business doesn't call for," Wang says. "Really take a close look at the security treatment of new technology and whether it opens you to risk and whether you're prepared to handle or accept it."

Jamie Gesswein wasn't willing to accept the risks that accompany social networking—not entirely any way. Gesswein, network security engineer for Children's Hospital of The King's Daughters in Norfolk, Va., says only a handful of public relations and marketing employees have access to social networking sites; the business case being that they need such access to monitor blogs and the like for mentions of the hospital.

WORKAROUNDS

You're the Last to Know

USERS ARE AHEAD OF IT WHEN IT COMES TO SIDE-STEPPING WEB 2.0 RESTRICTIONS.

DO YOU REALLY know the extent of what Web 2.0 sites are visited, or what tools are being installed on machines in your network? Your perception is probably counter to reality.

While more organizations are making a business case for the capabilities found in Web 2.0 applications, users for the most part aren't waiting for you to iron out your acceptable usage policies or lay out a list of permitted apps. They're forging ahead and using and installing a glut of Web 2.0 tools and applications such as peer-to-peer file sharing, Web conferencing and anonymiziers such as Tor, in addition to downloading user-generated applications from Facebook, MySpace and LinkedIn. These end-arounds are increasingly exposing companies to data leakage and malware infections.

Face Time Communications recently asked IT and security managers at more than 80 enterprises how many and which Web 2.0 apps they believed were running in their networks. Those estimates are far lower than reality. For example: 60 percent believed users were actively doing social networking; 54 percent thought P2P apps were installed and 15 percent were confident of the presence of anonymizers; when in fact there was 100 percent, or close to it, penetration of all of these tools and more, including Internet Protocol TV (IPTV), which streams mainstream television programming.

"Hackers are following people, and moving to Web 2.0," says Face Time VP of product marketing Frank Cabri. "Threats are moving in parallel."

And even when IT puts barriers in place–sites are blocked or restricted, or limits put on email files–users find other ways around them with the use of anonymizers or proxy servers such as Ultrasurf that bypass the corporate networks and policies banning visits to certain sites. Users wanting to move restricted data off a network can upload their hard drives to a Web-based storage service such as Dropbox or Megaupload. These services also support encryption.

"The problem is, IT is always the last one to know," says Palo Alto Networks VP of marketing Steve Mullaney. "The lack of visibility is the problem. You think you're stopping things by blocking MySpace, but younger people especially are going to be stopped for about two seconds. They're going to fire up Ultrasurf or use some encrypted proxy avoidance app that lets you do what you want." ›

–MICHAEL S. MIMOSO

"The biggest concerns were downloading malware and data leakage too," Gesswein says. Hospital staff aren't the only people with Internet access at the hospital; its young patients are allowed to bring in their laptops and access the Net via a guest wireless network. But even then, MySpace, Facebook and the like are blocked.

"We get a lot of calls from nurses and administrators asking us to allow access to kids to Facebook and MySpace, but we've stuck to our guns and not allowed it," Gesswein says. "I don't need a 7-year-old in the hospital accessing MySpace."

Organizations need to train users about which of their actions online pose the biggest risks.

"Don't click on links in Facebook, or on wikis or blogs," says Tim Roddy, senior director of product marketing at McAfee. "There's a real danger is you don't know who posted the content there. Most organizations have data security policies, but those need to be updated to include whether you can use web-based email to send information, or you can post to a blog. It's an awareness issue for employees because most data leakage isn't deliberate. Look at what's being posted; people shouldn't be blogging about their company—period."

A bigger driver is federal and industry regulation; for Children's Hospital of the King's Daughters, it's HIPAA compliance. With stringent watch on patient privacy in the health care industry, compliance helps drive the message home to upper management of the importance of data protection and get their backing to shut down as many egress points as possible.

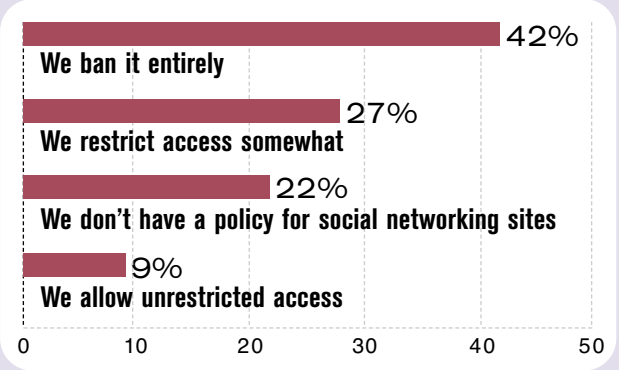
Still, deny-by-default isn't going to work forever. *Information Security* magazine's annual Priorities 2009 survey tends to back up this trend. More than 660 responded to a question about social networking, and 42 percent say they ban it entirely. Of the 58

SOCIAL NETWORKING POLICIES

Banned?

DOES YOUR COMPANY HAVE A POLICY FOR THE USE OF SOCIAL NETWORKING SITES?

Q Which best describes your policy for the use of social networking sites, e.g., Facebook and MySpace, for business?



SOURCE: Information Security's Priorities 2009 Survey; 662 respondents

EDITOR'S DESK

TABLE OF CONTENTS

STRETCHING YOUR DOLLAR

INTRUSION DETECTION OR PREVENTION?

CHOOSING A WEB APPLICATION FIREWALL

HOW TO SECURE WEB 2.0 TECHNOLOGY

percent that don't, only 9 percent said they allowed unrestricted access.

"In general, things are loosening up," Forrester's Wang says. "More people are saying it's useful for business purposes. And more people are allowing them to attract younger workers. It really depends on the company culture."

Clearly, a mix of technology and policy is the most sensible road to travel for many companies. Web security gateways that address not only antimalware, but URL and content filtering are being turned on social networking sites in order to catch private data such as credit card or Social Security numbers, or certain keywords that would indicate a corporate secret could be heading through the pipes onto the Web.

"The better weapon is to have the technology in place, but without policy, it would be moot," says Gesswein, who has a Sophos WS 1000 Web appliance installed on the hospital's network. The appliance, and others like it, inspects inbound and outbound traffic and compares it to policy, allows granular control over Web content and also includes an anonymizing proxy detection technology that sniffs out proxy servers more savvy users could use to sneak out confidential data through, for example, personal webmail accounts. "We have the ability to show the management what is going on in the network, what is being protected and how."

Gesswein struggles with that balance of providing access and enforcing policy. Doctors, like others in many industries, can collaborate online with peers via social networking sites. Medical collaboration sites and message boards, blogs and wikis are invaluable tools in speeding up patient care. Gesswein acknowledges that more staff members are also accessing information via personal devices such as BlackBerries and iPhones.

"The hardest thing is to have to keep telling myself that there has to be a balance. In a perfect world as a security person, everything is blocked, nothing is allowed. But in reality, we have to make money to stay alive. In order for them to make that money more efficiently, they need this technology in place, have access to information and be able to send and receive and talk to people more effectively. That balance between security and giving them this ability is tough. If you have to have this type of access and technology, let me work with you to figure out how I can protect the information and also at the same time, get you what you want."

MONITOR OUTBOUND CONTENT

Web 2.0 security isn't just about social networking and leaking secrets inadvertently on a blog post. Online productivity suites such as those afforded by Google apps are attractive no-cost options for organizations seeking free email, word processing, spreadsheets and document-sharing capabilities. Problems arise on these platforms from the lack of oversight, especially when they're used departmentally, or even by select individuals on a project.

Greenhill & Co., a small investment banking firm in New York, needed to get a handle on users accessing and moving documents on webmail services such as Gmail, Hotmail and others. John Shaffer, vice president of IT, says Sarbanes-Oxley auditors were looking at this risk and how it was being mitigated. Worse, he didn't want to see documents such as compensation spreadsheets leaking outside his organization via Gmail or Google docs.

"We had two choices: capture HTTP mail, or block it. We blocked it as opposed to

archiving external email," Shaffer says, adding that users were hurdling port-blocking firewalls by using SSL. The organization moved in Palo Alto Networks' PA series firewalls that consolidated threat protection and content filtering into one box. Shaffer had the visibility he needed to satisfy auditors and learn exactly what users were up to, especially over Gmail. He could also then set blocking policies per user via Active Directory.

"Data leakage was a big concern. We wanted to make sure people were not attaching spreadsheets," Shaffer says. "There are a number of ways to get data out of a network. We're at least making a best effort to get out to some. When we get audited and go through the whole Sarbanes-Oxley process, that's one of the things they're looking at."

While Gmail and Google Docs are free applications, enterprise versions provide some management and security capabilities that enterprises could use to rein in users via policy controls.

"If we are talking about a vendor that is providing collaboration services for corporations, you have to expect a very stringent policy control interface for me to say this type of document can be shared to this group, but not outside. Or, this document lives on a server for this long, but then is deleted," says Wang. "I haven't seen a lot of collaboration sites that offer this type of elaborate policy control interface to users. People like Google have to work on it. If they are trying to break into the enterprise, policy control is important."

Wang acknowledges that monitoring outbound content is difficult, but sees that trend spiking in a positive direction as more content security vendors acquire data leak prevention tools.

"There's a lot more going on around outbound data filtering," Wang says. "In the old days, it was all about filtering inbound email. Today, content filtering and webmail filtering is taking on more of a business context. We want to look at outbound content; what kind of mail you're sending out, attachments too, as well as Facebook and MySpace and what you're posting there. A lot of secure Web gateways have primitive abilities to recognize structured data. They're not as sophisticated enough to block corporate secrets, for example. That's in a fairly early stage. But that's the direction vendors are working hard toward."

The good news is that, yes, vendors and CISOs are looking at Web 2.0 security and the consequences of user behaviors online. Social networking presents security and productivity issues that run counter to growing business uses for these tools. Enterprises see a marketing value in Web 2.0 outlets such as Facebook, Twitter and LinkedIn. Younger people entering the workforce are used to having these sites and this kind of connectivity at their disposal, and expect it as part of their professional existence.

CISOs, as with any new online phenomenon, have to find that precious balance between security and productivity. Risk must be offset with a mix of policy and technology, and users must be educated so that important information isn't inadvertently leaked online.›

Michael S. Mimoso is Editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.