



Top 10 Threats to SME Data Security

(and what to do about them)

October 2008

*By Scott Pinzon, CISSP
Information Security Analyst, WatchGuard Technologies*

*Technical Editor: Corey Nachreiner, CISSP
Senior Network Security Analyst, WatchGuard Technologies*

Introduction

The mass media that covers IT often fixates on network security issues that are sensational, yet rare. If you follow IT issues too, you've probably seen the extensive reporting of a virus or a worm that refers to a notorious celebrity – even if in reality it is low-risk, and slow-spreading.

Sometimes the mainstream reporting on network security isn't even factual. In the second half of 2008, both Fox News¹ and the Sunday *Glasgow Herald*² reported on cases they touted as "the worst cyberheist ever." In each case, the subjects of the story denied the reported version. When objective observers asked for proof of the media claims, no further evidence was presented.

The upshot of all this sloppy reporting is that it's difficult to find reality-based, accurate reporting on what the network security threat really is today for the average business.

Since 1999, the WatchGuard® LiveSecurity® team (the folks who provide expert guidance and support for WatchGuard customers) has monitored emerging network security threats daily, with a special focus on issues that affect small to medium-sized enterprises (SMEs). When we spot an issue that could negatively impact SMEs, we alert our subscribers with email broadcasts. Because our subscribers are over-worked, time-constrained IT professionals, we alert only when we know an attack is not merely feasible, but likely. This

¹ FoxNews.com, October 10, 2008, "World Bank Under Cyber Siege in 'Unprecedented Crisis'," <http://www.foxnews.com/story/0,2933,435681,00.html>.

² Market Watch, August 24, 2008, "Best Western Responds to Sunday Herald Story Claiming Security Breach," <http://www.marketwatch.com/news/story/best-western-responds-sunday-herald/story.aspx?guid={A87F9682-AC67-4803-A135-B6ACF42C0956}&dist=hppr>.

emphasis on business context and practicality makes the LiveSecurity service nearly unique. Our approach is constantly refined by input from our tens of thousands of subscribers, field trips to customer sites, focus groups, and security-over-beer bull sessions.

As a result, we've developed a seasoned and practical perspective that differs from typical IT reporting. We've formed carefully considered conclusions on what types of data compromises most often occur in the real world. This paper lists the top 10 most common vectors of data compromise from our experience as security analysts for SMEs. We also suggest practical techniques and defenses to counter each vector.

If you are an experienced IT director or CSO, you should find few surprises here. Most of these topics are well-known in the trenches. But we consider them under-reported, for the simple reason that "normal" is not sexy. An average mistake or common misconfiguration does not often build into a fascinating headline that acts as a click magnet for online ad revenue. But if you're an administrator concerned about hardening your network against common problems, this is a more useful list than, say, "the top data breaches of all time."

We dedicate these observations and advice to helping you reach your Internet safety goals – so that you don't find your organization as the subject of the next sensationalized (and possibly exaggerated) data security headline.

Assumptions

Last year, WatchGuard passed the milestone of 500,000 security appliances installed. The majority of these installations occurred at businesses having between 20 and 1,000 networked users. When we describe common vulnerabilities and compromises, we have a particular network environment in mind. Generally speaking, we view a "typical" SME network as having the following qualities:

- **Average complexity.** Fewer than 3,000 networked devices
- **Predominantly Windows OS.** Most of the computers within one release earlier or later than XP SP2; Vista in the minority; a few Linux or Unix servers; up to 20% of users on Mac OS X
- **Many Microsoft business applications.** Heavy use of the Microsoft Office suite and Internet Explorer; Exchange server; SBS. Alternate software might be present, but does not dominate (for example, the IT staff might use Firefox but most users do not).
- **Public-facing web site.** Whether self-hosted or staged by an ISP, the organization has a web site, and the site accepts input from the public (e.g., in sales order forms or Web 2.0 features such as forum comments).
- **Porous perimeter.** What was formerly the network boundary is now amended to accept connections from business partners, remote laptops, kiosks, smart phones, and other mobile devices. Most of these connections are encrypted.
- **Wireless end users.** Whether at company headquarters or out on the road (probably both), many of the organization's end users connect via Wi-Fi.
- **Remote offices and telecommuters.** We assume this typical SME is not entirely officed in one building. The SME has at least a couple of permanent branch offices and many remote workers, such as a geographically dispersed sales force with employees connecting to HQ from home.
- **Understaffed IT department.** For various reasons, the IT team is at least one head count short of fully staffed, and as a result, much of the work is done in reactive mode.

In our minds, this is North America's typical small-to-medium enterprise network.

Top 10 Threats

While we feel confident that our list of threats reflects reality, our attempt to rank them by how frequently they occur is subjective. We believe that Threat # 1 happens far more often than Threat # 10, but the exact ranking is not really the point. Our goal was to identify the most common data security failures so that an IT staff can address them explicitly and intentionally.

In some of these ten items, we use the word "reckless." We intend the word as defined in the dictionary: "utterly unconcerned about the consequences of some action; without caution; careless."³ Today, the Internet must always be considered a hostile environment. To visit it carelessly is like visiting the toughest neighborhood in a big city after dark, flashing a roll of cash, and paying no attention to your surroundings. In short: unless you exercise caution, you're asking for trouble.

We list at least three mitigations or countermeasures for each threat. In the interest of saving your time, we tried not to repeat countermeasures. We could reasonably prescribe for the majority of these threats any of the following partial solutions:

- Monitor your logs regularly
- Install software patches promptly
- Train your users in security

If a particular countermeasure seems highly feasible in your particular environment, feel free to apply it across the board.

In hopes that this list helps you encourage your users to more thoughtful and cautious network usage, here are the threats our subscribers experience most often – and tips on defending your network against them.

Threat #10: Insider attacks

Verizon's Intrusion Response Team investigated 500 intrusions in 4 years and could attribute 18% of the breaches to corrupt insiders. Of that 18%, about half arose from the IT staff itself.⁴ (This indicates that senior management would do well to keep an eye on the IT staff.)

In our experience, insider attacks occur less frequently in SMEs than in major corporations. We attribute this to environmental constraints. If an SME CIO is disciplined and diligent, poor practices are much easier to log, notice, and correct on a small network than in a network with tens of thousands of users. There is also more likelihood in SMEs that every employee knows every other employee. It's harder to bury suspicious activities in a crowd when your co-workers are friends (or at least, not strangers). Plus, if corrupt people make up n percent of the global population, in raw numbers, a smaller user population contains fewer corrupt people.⁵

The flip side of this coin, though, is that a smaller staff more often entrusts sensitive duties to a single person, with no one co-responsible to provide checks and balances. A sensational illustration of the problem of entrusting too much to a single person played out in July 2008 when Terry Childs, a disgruntled contractor for the City of San Francisco, locked the City out of its own new multi-million dollar fiber WAN network.⁶ He

³ From dictionary.com, <http://dictionary.reference.com/browse/reckless>.

⁴ Summarized at http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm. For a PDF of the report, visit <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>.

⁵ For example, if we stipulate that 2% of all employees are corrupt enough to sell or abuse company data, a company of 10,000 employees has 200 potential traitors, while a company of 100 employees has only 2.

⁶ "S.F. officials locked out of computer network," <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11PIM5.DTL>.

could do so because no one else on staff fully understood the network architecture. Resolving the situation cost the city at least \$200,000 in contractor fees and paid overtime, and could add up to much more in the long run.⁷

Mitigating Inside Attacks

Implement the principle of dual control. Even if your key IT gal has earned your complete trust, can your company's work continue tomorrow if she gets hit by a bus? Implementing dual control means that for every key resource, you have a fallback. For example, you might choose to have one technician primarily responsible for configuring your Web, FTP, DNS, and SMTP servers. But at the very least, login credentials for those servers must be known or available to another person. Honest people tend to stay honest if they know that another observer could drop in at any time.

Formalize your hiring. If you're still hiring on the friend-of-a-friend method, perhaps it's time to step up to professional processes for hiring, including doing basic background checks. Depending on the type of data that resides in your network, criminal and credit checks might be appropriate, too. Always check the applicant's references – that practice is essentially free.

Reduce opportunity for mischief. Many insider compromises occur opportunistically. Promote the policy of locking computers into password-protected screensaver mode when leaving a desk unattended. Remind your users not to share their passwords with co-workers (middle-managers trying to empower their staffs typically are the worst at password overshare). Use firewalls internally to subdivide your network; for example, you can cordon off sensitive network segments such as R&D or HR to their own contained segments. Consider rearranging floor plans and furniture so that workspaces are open to more lines of sight, reducing chances for sneakiness. Resuscitate any security awareness campaigns that may have fallen by the wayside.

Threat # 9: Lack of contingency planning

Businesses that pride themselves on being nimble and responsive oftentimes achieve that speed by abandoning standardization, mature processes, and contingency planning. Many SMEs have found that a merely bad data failure or compromise turns disastrous when there is no Business Continuity Plan, Disaster Recovery Plan, Intrusion Response Policy, up-to-date backup system *from which you can actually restore*, or off-site storage. Each of these is considered a standard, base-requirement business practice, yet many SMEs treat them as "luxuries" and "overhead." Though such practices don't improve the bottom line immediately, your bottom line will experience much worse punishment if you procrastinate on contingency preparation until it's too late.

Mitigation for lack of planning

Policy development has a reputation for being painful, but it doesn't have to be that bad – nor all that expensive. Certainly if you have budget for it, hire an expert to help you develop sound information assurance methodologies. If you don't have much money to work with, leverage the good work others have done and modify it to fit your organization. These resources can help show you the way:

- "Producing Your Network Security Policy"
<http://www.watchguard.com/press/whitepapers.asp>
A common-sense approach that makes policy easier to draft, maintain, and enforce, using in-house expertise

⁷ "Tab for lockup of San Francisco's WAN may reach \$1M,"
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=326239>.

- The SANS Security Policy Project
<http://www.sans.org/resources/policies/>
Free resources, including sample policies and policy templates; deployment guidelines
- Internet Security Policy: A Technical Guide
<http://www.rxn.com/services/faq/internet/ISPTG.html>
Developed by Barbara Guttman and Robert Bagwill for the US National Institute of Standards and Technology (NIST), this classic paper still applies

Threat # 8: Poor configuration leading to compromise

Inexperienced or underfunded SMEs often install routers, switches, and other networking gear without involving anyone who understands the security ramifications of each device. In this scenario, an amateur networking guy is just happy to get everything successfully sending data traffic back and forth. It doesn't occur to him that he should change the manufacturer's default username and password login credentials.

Hackers keep long, diligently maintained lists of default logins to virtually every networking device, from the most expensive switch to the cheapest printer.⁸ If the configuration hasn't been changed from its default, anyone capable of doing a basic Internet search could feasibly log into your network resources and take control.

Network settings must be chosen with diligence and care. On one hand, most vendors ship their products with wide-open default settings, in order to minimize calls for technical support. Even if you've bought very powerful network security gear, those powerful defenses might not be turned on by default. On the other hand, mucking about with settings you don't fully understand could turn *off* defenses, or put the device in an unsafe listening state. A lot of networking equipment uses terminology that is difficult to understand, or labels that improperly communicate what an option does. In Verizon Business's report on the causes of 500 real-world data breaches, 62% could be attributed to significant internal errors that caused or directly contributed to the breach.⁹ In short: configure, but configure with care.

Mitigation for poor configuration choices

Always change the default username and password when installing networked devices. This requires no expertise and has no downside (unless you forget the password). Your password should be at least 15 characters long; using a favorite phrase from a movie, song, or scripture works well. The login credentials should be recorded and stored in a password vault that at least one other administrator can access.

Perform an automated audit scan. If you can afford it, hiring a penetration-testing organization to audit your network is a sound idea. But if you can't afford to hire consultants, you probably *can* afford a one-time, automated scan of your network. And if even *that* surpasses your budget, get your hands on a free tool such as Nessus¹⁰ or Nmap¹¹ and find out what is connected to your network. There are many, many vulnerability management products on the market at all price points. Regular use of one or more of them should be part of your network maintenance routine.

⁸ One example, maintained by a German hacker collective, can be found at <http://www.phenoelit-us.org/dpl/dpl.html>. Many such password lists exist.

⁹ Verizon Business RISK Team, "2008 Data Breach Investigations Report," www.verizonbusiness.com/resources/security/databreachreport.pdf. For a snappy summary, see http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm.

¹⁰ Nessus is vulnerability scanning software, and may or may not be free to you, depending on how you use it. For more information, start with the Wikipedia entry: [http://en.wikipedia.org/wiki/Nessus_\(software\)](http://en.wikipedia.org/wiki/Nessus_(software)).

¹¹ Nmap, short for "network mapper," is available as a free download: <http://nmap.org/>.

Have a consultant check you out. If you can tell you're in over your head when you try to configure a device, get expert help. Your ISP can probably recommend qualified consultants. So can your WatchGuard reseller.

Select solutions that are easy to use. When you add to your network, take advantage of free trials and hands-on demos. All SMEs love a bargain, but give extra consideration to products that make tasks understandable and easy. Getting a great price for gear you can't understand is a false economy.

Threat # 7: Reckless use of hotel networks and kiosks

Virtually every business has at least one or two (if not a hundred) road warriors attending industry events, visiting prospective customers, and meeting with clients. These employees most often work from laptop computers.

Hotel networks are notoriously lousy with worms, viruses, spyware and malware, and are often run with poor security practices overall.¹² Public kiosks make a convenient place for an attacker to leave a keylogger, just to see what falls into his net. Laptops that don't have up-to-date personal firewall software, anti-virus, and anti-spyware can get compromised at kiosks. Then, the next time the employee attaches to the headquarters network, a smart attacker can use that compromised laptop as the first stepping-stone to penetrate your entire network.

Adding to the risk: in a survey commissioned by Fiberlink, one in four road warriors admitted to altering security settings or purposely delaying security updates on a laptop in order to get their work done.¹³

Traditional defenses can be rendered useless when the user literally carries the laptop around the gateway firewall, and connects from inside the Trusted zone.

Mitigating reckless use of hotel networks

Make sure your road warriors have comprehensive defenses on their computers. Any device that's going to roam the wild and then return to your network should have on board, at minimum, anti-virus, anti-spyware/malware, and a personal firewall. Make sure that these all updated regularly.

Set and enforce a policy forbidding employees from turning off defenses. Workers used to shifting for themselves on the road often conclude, accurately or inaccurately, that laptop defenses are preventing them from doing their jobs. Many workers then disable the defenses. That practice might "solve" a short-term problem, but it also puts their computers at much greater risk. If you have IT personnel on call, your policy should be that workers are never to turn off defenses unless they call and receive authorization from you. Many popular anti-virus solutions can be configured so that they cannot be turned off, even by a user with local administrator privileges; check for such capabilities in your current solution.

Install client integrity checks at headquarters. You can find a wide variety of products designed to check the integrity and security health of remote clients requesting access to your servers. Different products filter by differing criteria. For example, you can reject connection requests unless they come from trusted MAC or IP addresses. Other types of products will check that the requesting client is running the latest versions of anti-virus, anti-spyware, firewall, and so on. When trying to select an endpoint integrity product,

¹² A recent study of 147 hotels by Cornell University found inadequate security practices at many of them. 20% of the hotels still used hubs in their networks and did not encrypt traffic, meaning, any guest of the hotel with a packet sniffer could see whatever hotel network activity and web surfing any other guest on the same subnet was doing. For more, see the Web Admin Blog entry "Consider Your Hotel Network Hostile," (<http://www.webadminblog.com/index.php/2008/09/15/consider-your-hotel-networks-hostile/>) and Cornell's report, "Hotel Network Security: A Study of Computer Networks in U.S. Hotels," available at <http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-14928.html>.

¹³ Fiberlink commissioned Kelton Research, who surveyed 333 IT professionals on line. The results were written up in a white paper, available from Fiberlink: http://www.fiberlink.com/fiberlink/en-US/knowledge/whitepapers/Kelton_Research_Results.html.

investigate how it performs remediation: if the product determines that an attempted connection does not meet integrity checks, what does it do? Ideally, if the problem is outdated defenses on the client, your integrity-checking solution should fix the problem automatically.

Threat # 6: Reckless use of Wi-Fi hotspots

Public wireless hotspots carry all the same risks as hotel networks -- and then some. Attackers commonly put up an unsecured wireless access point which broadcasts itself as "Free Public Wi-Fi." Then they wait for a connection-starved road warrior to connect. With a packet sniffer enabled, the attacker can see everything the employee types, including logins. This attack is particularly nefarious because the attacker pulls the data out of the air, leaving *absolutely no trace* of compromise on the victim computer.

The breadth and scope of wireless attacks is quite wide. For example, attackers can simply sit in the parking lot of any retail establishment that offers a public Wi-Fi hotspot; fire up a wireless packet sniffer; and record everything that goes by, in real time. But in another wireless attack known as sidejacking,¹⁴ an attacker can capture the session ID provided to your employee when she logs onto her web mail account. Depending on the web mail site's settings, the attacker could replay the session ID as much as *six months later* and read your employee's web mail.

Mitigating reckless use of Wi-Fi

Teach users to always choose encrypted connections. If a road warrior is using a company-authorized computer to connect back to your network, have the user connect via a Virtual Private Network (VPN). This encrypts the data stream, so that even though eavesdroppers can still listen in wirelessly, what they receive is gibberish. In public hotspots, users should always select an encrypted connection where possible. You can tell which networks are encrypted because they require a password, and the user interface will usually show which encryption method is in use: WEP, WPA2, etc. In public spaces, this offers only scant protection, since the public can learn the network password. However, it stops the most casual wireless wardrivers.

Encourage users to select reputable hotspots. When you're on the road and desperate for an Internet connection, you can find yourself in some pretty sketchy venues.¹⁵ Who knows what security practices they follow at Gung Lee's Smoke/Lotto/Manicure and Internet Café? Speaking very generally, a Wi-Fi hotspot at a global franchise such as McDonald's¹⁶ or Starbucks¹⁷ will have been built with customer safety in mind, and the store cares about its business reputation. Teach your staff to select known and quality hotspots whenever possible.

Teach users to prefer wired connections. Recent advances in cracking wireless encryption algorithms have dramatically decreased the amount of time attackers require to decrypt wireless transmissions.¹⁸ These recent innovations have led some security experts to recommend, when data is truly sensitive, not to trust wireless connections at all. Even on a wired connection, data is still more secure using a VPN.

For further mitigation against public W-Fi threats, follow the tips under Threat # 7, "Mitigating reckless use of hotel networks."

¹⁴ For details, see our video, "What is a sidejacking attack?" at <http://www.youtube.com/watch?v=nFNFa-48lpI>

¹⁵ Or doing odd things such as holding your laptop out the window to find the wireless signal. *CIO*, August 20, 2008, "20 Crazy Things People Do to Get Wi-Fi Connections,"

http://www.cio.com/article/445070/Crazy_Things_People_Do_to_Get_Wi-Fi_Connections?page=1.

¹⁶ McDonald's statement of wireless policy: http://www.mcdonalds.com/wireless/general_info.html.

¹⁷ Details of Starbucks' wireless offering: <http://www.starbucks.com/retail/wireless.asp>.

¹⁸ *The Register*, October 10 2008, "Turbo-charged wireless hacks threaten networks,"

http://www.theregister.co.uk/2008/10/10/graphics_card_wireless_hacking/.

Threat #5: Data lost on a portable device

Much sensitive data is compromised every year when workers accidentally leave a smart phone in a taxi, a USB stick in a hotel room, or a laptop on a commuter train. Does this happen often? The British government lost 747 laptops in four years.¹⁹

Setting aside employee negligence, sometimes devices are stolen: In Australia, 200,000 phones are stolen per year, or roughly one every three minutes.²⁰ In the UK, 2 million mobile phones are stolen per year, or, one every twelve seconds.²¹

In short, when the topic is data stored on small devices, it's wiser for administrators to stop thinking about what they'll do "if that device ever gets lost..." and instead, think, "*when* it gets lost..."

Mitigating data lost on portable devices

Teach users to proactively defend physical gear. Most robberies are opportunistic. Typical scenario: Alice's smart phone is in her purse. She's sitting in a coffee house and she decides her coffee needs more cream. She guesses it will be safe to leave her purse unattended during the few seconds it takes to cross to the counter where the cream is. The moment Alice stands and turns her back, a fleet-footed thief can silently snag the purse and flee. Even if Alice had the disposition and stamina to give chase, how could she, in business clothes and pumps? Most robberies can be prevented by refusing to put the device at risk, even briefly.

Company policy should require mobile devices to be password-protected. Most mobile devices offer the option of encrypting all user data on the device, and/or requiring a password in order to access the data. Users typically view such measures as drags on their productivity, and disable them. Your policy should require the use of available security measures, and detail serious consequences for employees caught ignoring the policy. Functionally, this is unenforceable. But a percentage of true believers will follow the policy. And it means you're covered and have the right to act if a flagrant abuse of the policy comes to light.

Manage mobile devices centrally. As technological reinforcement of the policy described above, consider investing in servers and software that centrally manage mobile devices. RIM's Blackberry Enterprise Server can help you ensure transmissions are encrypted; and if an employee notifies you of a lost phone, you can remotely wipe data from the lost Blackberry. You can also centrally enforce password access and password length on the devices, lock out Bluetooth connections, and more. For devices that run Windows Mobile 5.0, use the Messaging and Security Features pack and ActiveSync to enable device-wipe features. Even the risky iPhone can beef up its security a bit, though not centrally.²² These steps go a long way toward minimizing the negative impacts of lost devices.

Invest in encrypted USB flash drives. USB thumb drives, similar in size to an AA battery, are wildly popular and frequently lost. If you authorize company use of USB flash drives, spend the extra money to get the encrypted kind. Compared to a data breach, it's cheap insurance. Such drives²³ keep all their contents strongly

¹⁹ Asiaone, July 19, 2008, "British ministry admits loss of 747 laptops, secret data files," <http://www.asiaone.com/Digital/News/Story/A1Story20080719-77633.html>.

²⁰ Decoder, August 2008, "Mobile Phone Theft. What can be done?," <http://www.decoder.com.au/2008/08/06/mobile-phone-theft-what-can-be-done/>.

²¹ CNET Australia, May 10, 2007, "Lost mobile phones: a survival guide," <http://www.cnet.com.au/mobilephones/phones/0,239025953,339276173,00.htm>.

²² For details, refer to "Six Essential Apple iPhone Security Tips," CIO, October 7, 2008; http://www.cio.com/article/453280/Six_Essential_Apple_iPhone_Security_Tips?page=1.

²³ For example, the Kingston Data Traveler Elite Privacy Edition flash drive encrypts all its contents with 128-bit AES and requires a password to decrypt them. Brute force attacks fail, because after 25 consecutive failed password attempts, the drive destroys the data it contains. <http://www.engadget.com/2006/03/16/kingston-data-traveler-elite-privacy-edition-co-self-destructing/>.

encrypted. The legitimate user merely has to enter a password to go about business as usual. But if the device is lost or stolen and an attacker tries to guess the password, a number of consecutive wrong login attempts triggers data destruction. Many security professionals speak highly of Ironkey products, and a search on "secure USB flash drive" will show you many additional options.

Train your users in data security. Viewing your user community as willful laggards becomes a self-fulfilling prophecy. Instead, equip them to handle portable data with savvy. According to a survey from the Computing Technology Industry Association (CompTIA), when organizations instituted training for remote workers, 92% of these organizations said the number of major security breaches were reduced.²⁴

Threat #4: Web server compromise

Almost every SME today has a web site, and almost every web site has application code customized uniquely for the organization that runs the site. The most common botnet attack today is against web sites; and the fatal flaw in most web sites is poorly-written custom application code. Attackers have compromised hundreds of thousands of servers in a single stroke with automated SQL injection attacks.²⁵ Legitimate sites are then caused to serve malware, thus unwittingly spreading the bot master's empire. Legitimate sites that have suffered these attacks and wound up serving malware to their customers include those of Snapple, the City of San Francisco,²⁶ Sony Playstation,²⁷ and the British government.²⁸

Mitigating web server compromise

Audit your web app code. If (for instance) a web form has a field where a visitor is intended to supply a phone number, the web application should be written to discard excess characters. If the code is not written in this way, an attacker can submit an entire executable script of thousands of characters in a field that need accept only 14 characters. Web app code should also fail shut when handling errors; in other words, if the program doesn't know what to do with data or a command, it should reject it, not process it. These are just two examples of the security issues that commonly go wrong for the SME that is too frugal or too rushed to audit web site code.

Input validation is the fancy term for making sure your web apps will not accept malicious data or commands from the Internet. Allowing for your budget, seek the best code auditing solution you can afford (whether a team of experts or an automated tool), with emphasis on finding out whether your code does proper input validation.

Don't trust your web server. Any web server that the public can access should not reside within the Trusted segments of your network. Keep such web servers in the "DMZ," and minimize the number and type of connections from the server to more trusted internal resources.

Use a firewall that can filter HTTP and HTTPS traffic. If your firewall performs little more than stateful packet-filtering, it is focused primarily on packet headers rather than packet payloads. That's similar to hiring someone to inspect your mail for letter-bombs, but he only examines the outside of the envelopes. Seek a gateway solution that can catch malicious HTTP traffic. It should be able to inspect content, not just headers, by examining traffic both heuristically and against a list of "known bad" signatures.

²⁴ CIO, May 21, 2008, "Mobile-Related Security Threats on the Rise,"

http://www.cio.com/article/364113/Mobile_Related_Security_Threats_On_the_Rise.

²⁵ A botnet called Asprox provides an example of this. For details, see Secureworks' analysis from May 2008:

<http://www.secureworks.com/research/threats/danmecasprox/?threat=danmecasprox>

²⁶

http://securitywatch.eweek.com/exploits_and_attacks/huge_volumes_of_bigtime_sites_hacked_via_asprox_attacks.html

²⁷ <http://blogs.zdnet.com/security/?p=1394&tag=rbxccnbzd1>.

²⁸ <http://security.itproportal.com/articles/2008/07/24/super-malware-asprox-takes-uk-storm-targets-government-websites/>

Threat #3: Reckless web surfing by employees

As recently as five years ago, the average person could discern when he or she was surfing to a shady area of the Internet. You usually didn't get infected with malware unless you visited a porn site, a gambling site, or some sort of low-rent, illicit web page. No more. A 2006 study by the University of Washington²⁹ found that the sites that spread the most malware were (in order)

1. Celebrity fan sites (such as the type that give breathless updates on the follies of Paris Hilton and Britney Spears)
2. Casual gaming sites (where you can play checkers or Battleship against a stranger)
3. Porn sites (coming in at a surprising third place)

Employees who surf to non-business-related sites end up inviting malware into the corporate network. The unhappy payoff can include bot clients, trojans, spyware, keyloggers, spambots – pretty much the entire gamut of malware.

Since the UW's 2006 study, social networking sites such as MySpace and Facebook have taken the lead as veritable cesspools of spam, trojans, and spyware – not to mention crash-prone apps and, with video involved, avalanches of non-business-related, bandwidth-hogging traffic³⁰. Click-happy users mean no harm, but they cause it anyway.

Mitigating reckless web surfing

Gather data on your company's current web habits. The computers and Internet connection at your company headquarters are often more robust than the equipment your employees have at home. As a result, they usually prefer your network over their own for shopping, paying bills online, and more. Employees often consider this a soft benefit of working for you.

But you might be surprised at the unreasonable lengths some employees go to. If you have not looked at outbound HTTP traffic in your logs, you should. Clients following our advice have discovered that employees surf porn at lunch; run their own small business sites from the company's network; download pirate software via company servers; and more. Get some empirical evidence of how much cyberslacking is occurring within your user community; then you can respond appropriately, based on facts.

Adopt a stricter policy. Because the amount of hostile traffic on the Internet has climbed dramatically in the last three years, liberal web policies need to be reconsidered. The data you gather on current web traffic might provide good reason to override your employee's protests and implement new, safer policies. Depending on what's appropriate to your business environment, consider revising your Acceptable Use Policy to rope off entire swaths of the Web. Think big and take back your network: if you'll be safer implementing "no sports, no celebrity sites, no political blogs, no [fill in the blank];" consider banning anything that doesn't support your institutional mission.

Implement web content filtering. You can put technological enforcement behind your new tough policy using web filtering software such as the WebBlocker service from WatchGuard. Web filtering solutions maintain databases (updated daily) of blocked URLs in scores of categories. More categories mean more nuance. If, for example, you run a medical clinic, you might need to allow access to some sports sites related to injuries your patients sustain; but with URL filtering, you can still block Fantasy Football and the NFL.

²⁹ University of Washington News, February 2006, "Spyware poses a significant threat on the Net," <http://www.uwnews.org/article.asp?articleID=22331>.

³⁰ WatchGuard Blogs, October 2008, "Brace your users for anti-social networking," <http://blogs.watchguard.com/2008/10/brace-your-users-for-anti-social.html>.

As with many of these Top Threats, security awareness training is part of the mitigation. Consider making it mandatory for every employee to view a training video such as our free "Spyware: Think Before You Click"³¹.

Threat #2: Malicious HTML email

The vast majority of attackers who choose email as their primary vector have stopped sending emails with malicious attachments. (That's so 2003!) The most common email attack now arrives as an HTML email that links to a malicious, booby-trapped site. One wrong click can trigger a drive-by download.³² The hazards are the same as in Threat # 3, "Reckless web surfing;" but the attacker uses a slightly different vector to get the victim to his malicious website.

Mitigating malicious HTML email

Implement aggressive spam filtering. Take advantage of the plethora of excellent spam filtering products, and layer different approaches. You can filter spam at the desktop of the recipient; at your mail server; and at the gateway to your network. You can do it via Bayesian filters, character strings, regular expressions, and recurrent pattern detection. Ask a trusted advisor to help you craft the combination of defenses that is best for you. Since more than 80% of all emails are spam,³³ we recommend solutions that drop unwanted email at your gateway, before the spam burdens your mail server. That frees up more server resources for handling legitimate email.

Implement an outbound web proxy. Some administrators set up their LAN so that all HTTP requests and responses get re-directed to a web proxy server. This technique provides a single choke-point where all web traffic can be monitored for appropriateness. The web proxy won't catch an inbound malicious email, but if a user on your network clicks a link in that HTML email, doing so generates an HTTP request that the web proxy can catch. This provides two advantages. First, the majority of malware is not very sophisticated, and simply won't work if a web proxy interrupts the HTML request – the link won't know how to "phone home." Second, the proxy provides an excellent opportunity to scan or filter HTTP and stop questionable traffic. If the user's HTTP request never makes it to the attacker's booby-trapped web site, the trap is never sprung, and your user and your network do not become the victim.

Raise user awareness about email security. Malicious email grows increasingly deceptive year after year. The days are gone when you can count on recognizing spam because it is spelled poorly. Users must be made aware that criminals might send them email. Users also need examples of what dangerous emails look like. Implement periodic training and reminders. For starters, try showing our free security awareness video, "Bud Has Mail."³⁴

Threat #1: Automated exploit of a known vulnerability

Verizon's *2008 Data Breach Investigations Report* compiles factual evidence from more than 500 data breaches, occurring over the course of four years. Verizon's RISK Team was able to verify that 73% of the breaches occurred from external sources (as opposed to insider betrayal, or sloppiness on the part of a business partner).

In all but rare cases, the typical SME will not be the target of a focused, purposeful attack by a malicious hacker or criminal collective. Most of the threat to a typical small business comes from the tides of automated attacks scanning the Internet daily. The Open Web Application Security Project (OWASP) characterizes such attacks as

³¹ Available from Google Video at <http://video.google.com/videoplay?docid=-4094518401580008932>.

³² If this term is unfamiliar to you, see our video, "What Is a Drive-by Download?" at <http://video.google.com/videoplay?docid=-3351512772400238297&ei=DubvSOTxOpH8qAPUjH4Dw&q=Corev+Nachreiner>.

³³ CommTouch Year-End Email Threat Report, http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=983&cat_id=1.

³⁴ Preview and free download available at <http://www.watchguard.com/budhasmail>.

"non-targeted,"³⁵ because they attempt to compromise any computers having security holes the attacker knows how to exploit. The vast majority of automated attacks on the Internet try to exploit holes in Windows.

Microsoft provides patches every month, but short-staffed SMEs may fail to install the patches. Installing patches can be daunting. Sometimes the patch itself introduces new problems to the network, so all patches must be tested before they are deployed. Yet, patching is essential.

Consider these contrasting statistics. There are botnets right now successfully exploiting flaws that Microsoft patched *four years ago*.³⁶ On the other hand, in Verizon's investigations of 500 data breaches, there were zero cases of an attacker exploiting a vulnerability within 30 days of it being announced and patched. So statistically speaking, if you can patch a known vulnerability within 30 days of the vendor publishing the patch, you are likely to head off attacks.

Negligent SMEs commonly get victimized if they don't install Windows patches during the same month the patch is published. But your network contains much more than Microsoft products. Your patching routine needs to extend systematically to all the applications and OS components on your network.

Mitigating automated exploits

Invest in patch management. For any LAN larger than a simple home network, it's risky to patch on an ad hoc basis. Patch management software will help you scan your network, identify missing patches and software updates, and distribute patches from a central console, greatly increasing your chance of having your entire network up to date. For a Windows-based LAN, the most applauded patch management software comes from Shavlik³⁷. However, if you search on "patch management software," you can find solutions at all price points.

Build an inexpensive test network. Some vendors offer rock-solid patches and updates; others (especially those with complex products), issue patches where the cure is worse than the disease. Even reputable companies can slip up. Therefore, we recommend installing a patch on a test system and seeing how it behaves before deploying it throughout your network. If you don't have a test network now, the next time you replace outmoded desktop computers and servers, hang onto them and dedicate them to being your test network. Alternatively, if you have one spare computer that is robust, you can affordably set up a "test network" on it by using virtualization products to install virtual servers and virtual PCs. You can search on "virtualization products" to learn more about products from VMware, Microsoft, Citrix, and many, many others.

Keep an eye on the vendor forums that mean the most to you. Any software application or networking device that is critical to your ability to stay in business should be represented on the short list of websites you check every day. User communities, official blogs, and support forums are often the first to report on new vulnerabilities. Problems caused by faulty patches generally come to light within two days of the patch or upgrade release as relevant forums light up with urgent discussions. By watching them, you can learn when the majority of users deem it wise to upgrade.

Emphasize thoroughness over speed. "Patch promptly" has been preached so much that some organizations turn patching into a fire drill. You don't need to work your staff overtime or rush them. It's more important to verify that patches or updates are stable and that they don't break any custom applications your organization runs. You want to make sure you patch every vulnerability you can, so take a systematic approach. As long as you plan the work and work the plan, the odds are you will get to your security holes before hackers do, and without overlooking an obscure yet important upgrade.

³⁵ The highly respected OWASP lists "non-target specific" attacks as the number one threat agent on their wiki: http://www.owasp.org/index.php/Category:Threat_Agent .

³⁶ For substantiating details for this claim, search the Web for bots by name. Examples include Rxbot (aka Rbot), Gaobot, and SDbot.

³⁷ Shavlik Netchk has enjoyed wide support from networking professionals for years; for details, see <http://www.shavlik.com/netchk-protect.aspx> .

Minimize what's installed on your network. Most end users have no concept of ongoing maintenance, or of the unintended side-effects possible when applications interact. The more applications and software utilities you have on your network, the more opportunities you create for attackers to find a weak spot. Seek to standardize as much as possible on a single corporate hard drive image with a set suite of apps, tools, and defenses. For example, if workers can get their needs met with Windows Media Player, there's extra risk but no extra upside to also allowing Quicktime, WinAmp, RealPlayer, and DivX on your network. When departments ask for exceptions, require a business justification. In essence, this tip is saying *do* put all your eggs in one basket – but then guard that basket!

Consider alternatives to "hole-y" software. Certain software applications attract attackers, in part because of their popularity; in part, because they have known vulnerabilities. If these oft-attacked packages are not vitally integrated into your network environment, consider replacing them with less attacked or more secure alternatives. For example, Internet Explorer has long been a favorite target of mass exploits. Consider switching your standard corporate browser to Mozilla Firefox, running the plug-in called NoScript. If your users are just as happy with Mac OS X as they are Windows, currently there are far fewer trojans and attacks for OS X. Switching might be a viable alternative for you.

However, don't fall for security by obscurity. Today's attackers follow the money. If today's "safe" software gains enough market share to lure attackers, it might become the next big target. If you switch a common application for a less common one, it should be because the less-common app has genuine security advantages, not because attackers haven't focused on it yet.

Conclusion

To recap, we believe that realistically, the top ten threats to SMEs are:

10. Insider attacks
9. Lack of contingency planning
8. Poor network configuration leading to compromise
7. Reckless use of hotel networks and kiosks
6. Reckless use of Wi-Fi hot spots
5. Data lost on a portable device
4. Web server compromise
3. Reckless web surfing by employees
2. Malicious HTML email
1. Automated exploit of a known vulnerability

All of these attack vectors are well-known to security professionals. Mature processes, techniques, and technologies are available to help you defend against them. Although on some days it might feel like the bad guys are winning, through diligence and persistent effort, you can harden your network against attacks. Thousands of network administrators run for years at a time without any compromises or intrusions. We hope this paper contributes to your being counted among those savvy administrators. For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilize mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner.

For more information

In addition to the countermeasures we've suggested above, a diligent network administrator might want to examine the range of security solutions that WatchGuard Technologies offers. Our Extensible Threat Management (XTM) gateway security appliances go a long way to solving nine of the ten threats listed herein. (Sadly, our appliances cannot stop your employees from losing portable devices.) But our solutions *can* help you secure your wireless network, check the integrity of clients requesting access to your network, filter spam, proxy web services, minimize insider threats, create VPNs, and much more. For details, visit www.watchguard.com or talk to your WatchGuard reseller.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest solution – the WatchGuard XTM 1050 – provides high performance and fully extensible, enterprise-grade security at an affordable price. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66594_110508