Top 10 Threats to SME Data Security

The following article is excerpted from "Top 10 Threats to SME Data Security (and what to do about them)," a white paper written by Scott Pinzon, CISSP, of the WatchGuard® LiveSecurity® team. This summary lists the ten threats and one countermeasure for each. For more details on how we selected the threats we did, what type of network we are addressing, and at least two more countermeasures for each threat, download a free copy of the full white paper at www.watchguard.com/whitepapers.

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 has monitored emerging network security threats every day, with a special focus on issues that affect small to medium sized enterprises (SMEs). When we spot an issue that could impact SMEs negatively, we alert our subscribers with email broadcasts. Because our subscribers are time-constrained, over-worked IT professionals, we alert only when we know an attack is not merely feasible, but likely. This emphasis on business context and practicality makes our service nearly unique. This 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.

The result: this paper lists the top 10 most common vectors of data compromise in our experience as security analysts for SMEs. We also suggest practical techniques and defenses to counter each vector.

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.[1]

Implement the principle of dual control. 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 and SMTP servers. But at the very least, login credentials for those servers must be known or available to another person.

Threat # 9: Lack of contingency

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.

Mitigation for lack of planning

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. The SANS Security Policy Project offers free templates and other resources that can help you write your own policies. For more, visit http://www.sans.org/resources/policies/.

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.

Mitigation for poor configuration choices

Perform an automated vulnerability audit scan. If you can't afford to hire consultants, you probably *can* afford a one-time, automated scan of your network. There are many, many "vulnerability management" products on the market at all price points. Regular use of them should be part of your network maintenance routine.

---

[1] 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.

Threat # 7: Reckless use of hotel networks and kiosks

Hotel networks are notoriously lousy with viruses, worms, spyware, and malware, and are often run with poor security practices overall. 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 on the road. 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

Set and enforce a policy forbidding employees from turning off defenses. According to a survey commissioned by Fiberlink, 1 in 4 "road warriors" admitted to altering or disabling security settings on their laptops. 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.

Threat # 6: Reckless use of Wi-Fi hot spots

Public wireless hot spots 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 WiFi." 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.

Mitigating reckless use of Wi-Fi

Teach users to always choose encrypted connections. Have them connect via a Virtual Private Network (VPN). This encrypts the data stream, so that even if eavesdroppers listen in wirelessly, what they receive is gibberish.

Threat # 5: Data lost on a portable device

Much sensitive data is compromised every year when workers accidentally leave their smart phone in a taxi, their USB stick in a hotel room, or their laptop on a commuter train. When data is 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

Manage mobile devices centrally. 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. Such steps go a long way toward minimizing the negative impact of lost devices.

Threat # 4: Web server compromise

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. Legitimate sites are then caused to serve malware, thus unwittingly spreading the bot master's empire.

Mitigating web server compromise

Audit your web app code. If (for instance) a Web form has a field for a visitor to supply a phone number, the web application should discard excess characters. If the web application doesn't know what to do with data or a command, it should reject it, not process it. 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.

Threat # 3: Reckless web surfing by employees

A 2006 study by the University of Washington found that the sites that spread the most spyware were (in order)

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

Social networking sites such as MySpace and Facebook have taken the lead as virtual cesspools of spam, trojans, and spyware. Employees who surf to non-business-related sites end up inviting into the corporate network bot clients, Trojans, spyware, keyloggers, spambots… the entire gamut of malware.

Mitigating reckless web surfing

Implement web content filtering. Use web filtering software such as WatchGuard's WebBlocker. Web filtering solutions maintain databases (updated daily) of blocked URLs in scores of categories. More categories means more nuance. Such tools help you enforce your Acceptable Use Policy with technology.

Threat # 2: Malicious HTML email

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. The hazards are the same as in Threat # 3, "Reckless web surfing;" but the attacker uses email to get the victim to his malicious website.

Mitigating malicious HTML email

Implement an outbound web proxy. You can set up your LAN so that all HTTP requests and responses redirect to a web proxy server, which 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, that will generate an HTTP request that the web proxy can catch. If the user's HTTP request never gets to the attacker's booby-trapped web site, your user does not become the victim.

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 4 years. Verizon's RISK Team found that 73% of the breaches occurred from external sources. Negligent SMEs 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. 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.

Build an inexpensive test network. 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.

Conclusion

The countermeasures we've suggested above can go a long way in mitigating your risk and protecting your network. But these are only a sampling of the steps that a diligent IT administrator could implement to increase network security. For more practical advice on hardening your network against common problems, download a free copy of the complete **Top Ten Security Threats for SMEs (and what to do about them)** white paper from the WatchGuard web site.

WatchGuard® provides extensible threat management (XTM) gateway security appliances that address nine of the ten threats listed herein. (Sadly, our appliances cannot stop your employees from losing portable devices.) We *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 information about WatchGuard security solutions and the protection they provide against botnets and other network threats, visit us at www.watchguard.com or contact your reseller.