Tech Brief

Four basic and effective defensive measures against cybercrime

- Cybercriminals target small businesses because they are often an easier target.
- Sixty percent of security breaches in 2011 could have been prevented with basic security.
- Data and network audits are a simple way to get started with a security policy.

By Stephen Cobb, ESET Security Evangelist

Evidence that criminals are targeting the computer systems of small businesses continues to mount. The *Wall Street Journal* recently drew attention to the way cybercriminals are sniffing out vulnerable firms. The article highlighted the fact that about 72 percent of the 855 data breaches worldwide last year that were analyzed in Verizon's Data Breach Investigation Report were at companies with 100 or fewer employees.

Many small businesses don't realize that, regardless of location, they can be the target of cyberattacks such as the one ESET researchers recently discovered in Peru (check out the ESET white paper in PDF form here). In this case, the bad guys deployed technology that could silently steal AutoCAD drawings, files that often encapsulate the intellectual output of small companies such as architectural and engineering firms.

There is also mounting evidence that small law firms working on big cases are increasingly being targeted by parties with an interest in a specific case. According to Trent Teyema, FBI assistant special agent in charge of cybercrimes in the agency's Washington field office: "We have seen over the last three years an increase in the targeting of law firms." And here's Stewart Baker, former assistant secretary for policy at the Department of Homeland Security: " to believe that foreign governments are breaking into American law firm networks."

With that in mind, the following are four tips for small businesses looking to prevent cyberattacks, bearing in mind that there is a lot more to each of these than we have room for in this tech brief:

1. Know what you are defending: Many small firms don't have a clear picture of their digital assets or where they reside. Have a session where management and IT review the following (even if the sum total of management and IT at your firm is only two people):

a. data that comes into the firm (e.g., work orders, customer information),

b. data the firm creates and stores (e.g., project designs or research notes), and

c. data that is allowed or required to leave the firm (e.g., reports to clients).

> "There is every reason to believe that foreign governments are breaking into American law firm networks," says former assistant secretary for policy at the Department of Homeland Security.

ESET BUSINESS SOLUTIONS

ESET Endpoint Solutions

ESET Endpoint Antivirus (Windows/Mac*/ Linux*)
Antivirus / Antispyware

ESET Endpoint Security (Windows)
Antivirus / Antispyware / Firewall / Antispam

ESET Mobile Security (Windows Mobile/Symbian)
Antivirus / Antispyware / Firewall / Antispam

ESET Server Solutions

ESET Mail Security (Windows/Linux)
Antivirus / Antispyware / Antispam

ESET File Security (Windows/Linux)
Antivirus / Antispyware

ESET Gateway Security (Linux)
Antivirus / Antispyware

*ESET NOD32 Antivirus Business Edition Mac OS X,
ESET NOD32 Antivirus 4 Business Edition for Linux

Mac

> A 2011 Verizon Data Breach Investigation Report found that more than 90 percent of breaches were avoidable if security measures classified as basic or moderate had been in place.

In addition to this "data audit," you need to perform a "network audit" to make sure you know what equipment is on your network and what devices are connecting to the Internet and/or phone lines (e.g., is the sales team logging in to the office network from the road to access customer records, is your photocopier calling home to the manufacturer). When you get a clear picture of where the sensitive data is, and who has access to it, then you can put some rules in place.

2. Have rules:
A written information security policy or plan is essential for all small businesses these days and may even be required by law (e.g., if you handle information about health matters or citizens of the state of Massachusetts). There can be a big upside to putting such a plan or policy in place because many larger firms are requiring them from the smaller firms that are their suppliers. In other words, you could beat out the competition for a contract if you have a security policy in place and they don't. A few months ago we recorded a webcast on cybersecurity policy for SMBs that you might find useful (registration required).

3. Enforce the rules:
The catch with security policy is that you need to enforce it. That includes sanctioning people who violate the rules but also educating all your employees about what the rules are. It is not unusual for a large company to insist that an approved vendor or contractor show evidence of a program of security awareness for its employees, even if they are a small firm. You can find more about this topic in these slides: Cybersecurity Policies and Best Practices: Protecting small firms, large firms, and professional services from malware and other cyber-threats (PDF).

4. Start with stronger passwords:
This sounds like a very low-tech tip, but it has a high reward. Educate employees on what constitutes a strong password. Make them use strong passwords on all systems, including smartphones and tablets. Change the default password on routers and point-of-sale equipment. The good news here is that more than 60 percent of all data breaches in 2011 could have been prevented with cheap and basic security measures. That's according to the Verizon Data Breach Investigation Report, which found that more than 90 percent of breaches were avoidable if security measures classified as basic or moderate had been in place.

As for responding to an incident, being prepared is more than half the battle. A good first step is to know who in local law enforcement deals with cybercrime and also get to know your local FBI office. The latter should be ready and able to respond to major intellectual property cases or bank fraud. And the FBI now has access to an improved range of tools and resources if you are prepared to "make a federal case" out of an incident. The Federal Trade Commission has a useful page of tips for businesses that do suffer a data breach.

*Stay up to date with the latest Internet threats— visit **blog.eset.com***

*Protect your digital privacy with ESET. For more information on your security options, go to **eset.com***

ESET North America
610 West Ash Street
Suite 1700
San Diego, CA 92101

Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400

eset www.eset.com