INSURANCE JOURNAL

How Cybercriminals Attack Small Businesses — and 10 Ways to Stop Them

September 15, 2014

At a recent “Hacker Lab” event, “white hat” hackers revealed how cybercriminals work — and what businesses can do to protect themselves. The multimedia presentation used a simulated small business system to demonstrate how hackers choose their targets, how they enter the system and what they do post-infiltration.

The “Hacker Lab” was presented by HSB, a specialty insurer of data and information risks that is part of Munich Re, and Trail of Bits, a New York City-based cybersecurity firm. It was designed to provide risk mitigation resources for small business owners.

Key takeaways for small business owners included:

- Cybercriminals view small business both as a target and as a conduit to attack their clients.
- Small businesses must identify their assets and the data they have that’s valuable to others; keep only what is needed and use a dedicated device for financial activity that’s not used for email or social media.
- Most cyber-attacks enter a company through email and browsers. Businesses must take steps to secure both.

“No business is ‘too small’ for a hacker. All businesses are vulnerable,” according to Eric Cernak, vice president, strategic products, HSB.

INSURANCE JOURNAL

Small Businesses Hit With Data Breach Often Fail to Notify Customers

A study HSB conducted with the Ponemon Institute found that more than half of all small and mid-sized businesses experienced a data breach and nearly three-quarters can't restore all their data.

"The problem is big and growing. The good news is that businesses can take steps to protect themselves from destructive criminal intrusions," said Cernak.

Company Data Breach Now Costs $3.5M on Average

Dan Guido, Hacker in Residence at NYU Engineering and founder and chief executive officer of Trail of Bits, agreed that businesses need to get out ahead of the hackers.

"Reacting to new threats is too slow and too expensive. These days, you have to pre-empt criminal activity by thinking like a hacker and concentrating on the methods of attack," said Guido. "Fortunately, attackers are just as fallible as everyone else and they can be disrupted."

Alexander Sotirov, founder and chief technology officer, Trail of Bits, participated with Guido in the demonstration.

The "Hacker Lab" also featured a robust risk management discussion with Cernak and Tim Zeilman, vice president and counsel, strategic products, HSB, about ways to prevent a cyber-attack; the legal, financial and reputational costs of an attack; and what businesses must do if/when they're hacked. HSB and Trail of Bits provided the following risk-management tips:

10 Ways for Small Businesses to Prevent a Data Breach

1. Outsource payment processing. Avoid handling card data on your own. Reputable vendors, whether it's for Point-of-Sale or web payments, have dedicated security staff that can protect that data better than you can.

2. Separate social media from financial activity. Use a dedicated device for online banking. Use a different device for email and social media. Otherwise, just visiting one infected social site could compromise your banking machine and your savings account.

3. Think beyond passwords. Never reuse them and don't trust any website to store them securely. You can never tell when a website has already been hacked and your password has been exposed. Set up a two-factor authentication; this sends a secret code to your phone verifying your identity.

4. Educate and train employees. Establish a written policy about data security, and communicate it to all employees. Educate employees about what types of information are sensitive or confidential and what their responsibilities are to protect that data. Also, most scams and malicious attacks arrive through email so be sure your team is prepared and alerts others when they are received.

INSURANCE JOURNAL

5. Stay informed. Evaluate the entire chain of events in a potential attack. From assessing your email infrastructure to your users' responsiveness to your browser's vulnerability, identify where your organization is most at risk. Then, question the security posture of your business lines, vendors, suppliers or partners.

6. Stop transmission of data that is not encrypted. Mandate encryption of all data. This includes data at "rest" and "in motion". Also consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks; they may permit interception of data.

7. Secure your browser. With the growing popularity of watering holes – malicious code installed on trusted websites – how do you know which websites you can trust? Forget individual patches. Focus on keeping up to date with the latest version of your browser. Then, test your browser's configuration for weakness.

8. Secure your operating system. It's far easier to break into older operating systems like Windows XP or OS X 10.6. Take advantage of major security improvements baked into newer operating systems.

9. Secure your router. It connects your computer to the Internet. Make sure someone can't intercept all the data sent through it. It's important to set a strong admin password on your router and a WPA2 password on your Wi-Fi.

10. Secure your data. Whether you lose data to an accident or an attack, you'll always be glad to have a backup. Ideally, your backups should be encrypted and off-site in case there's a fire or burglary.