How to Protect Your Small Businesses Against Cyber Attacks

Dec 10, 2014

No business is 'too small' for a hacker. All are vulnerable.

– Eric Cernak, VP — Strategic Products, HSB

Hacker Lab, a world-leading IT security portal, which deals with hacking and defense strategies, recently showed how cyber criminals work and what small businesses can do to protect themselves (by White Hat Hackers). The organization used a multimedia presentation to demonstrate the hacker strategy of choosing their targets, their entering process into the system and what they can do after having been compromised.

The "Hacker Lab" was presented by Hartford Steam Boiler Inspection and Insurance Company (HSB), a specialty insurer of data and information risks (a part of Munich Re), and Trail of Bits, a New York City-based cyber security firm. The event was designed to provide risk management and mitigation resources for the small business owner.

Every Small Business is Vulnerable

Key takeaways for Small Business Owners included:

- Cyber criminals consider small entities as a target and a conduit to attack their clients as well.

- Small entities must identify their assets and the data they have that is valuable to others. They should keep only information that is needed. They should also use a dedicated device for financial activity that is not used for email or social media.
- Most cyber-attacks enter an organization through email and browsers. Entities must take necessary steps to secure both of these entry points.

Research conducted by HSB along with the Ponemon Institute showed that more than half of all small to mid-sized businesses have experienced a data breach, and nearly three-quarters are not able to 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,” Eric Cernak, VP for strategic products at HSB stated.

Another famous hacker, Dan Guido, resident at NYU Engineering and Founder/CEO of Trail of Bits, agreed to the fact that businesses need to get ahead of the hackers.

Hacker Lab also featured a discussion on risk management with Cernak and Tim Zeilman, featuring ways to prevent a cyber-attack; the legal, financial and reputational costs of an attack; and what small businesses must do if/when they’re hacked.

10 Steps Every Business Should Take

HSB and Trail of Bits provided the following risk-management tips:

1. Outsource payment processing

Try to avoid handling credit card data on your own. Reputable vendors (whether it is for Point-of-Sale or web payments) have assigned security staff who can protect that information better than any small business can.

2. Separate social media from financial activity

Use a dedicated and specific computer for online banking. Ensure you use a different device for email and social media. If you don’t, your banking machine and savings account could be compromised when visiting even just one infected social site.

3. Think beyond passwords

Never use the same password and do not trust any website to store them securely. You can never know when a site has already been hacked and your password has been compromised. Install two-factor authentication whenever available to send a secret code to your phone as an additional step to verify your identity.

4. Educate and train employees

Create and implement a written policy for data security. Communicate it to all employees. Educate them about which types of information are sensitive or confidential and what their responsibilities are to protect those pieces of information — be it large or small. Most scams and malicious attacks arrive through email, so be sure your team is able to identify suspicious emails and make sure they alert others in the organization when they are received.

5. Stay informed

Monitor the entire chain of events in a likely attack. From accessing your email infrastructure to your users’ responsiveness, to your browser’s vulnerability, identify which area of your organization is most at risk. Then, question the security posture of your business lines, vendors, suppliers or partners.

6. Stop sending data that is not encrypted

Ensure that data is encrypted on a regular basis. This may include data at “rest” and “in motion.” You will also need to consider encrypting email within your organization that contains personal information. Avoid using Wi-Fi networks, which may permit interception of data.

7. Secure your browser

With the growing popularity of watering holes (questionable code installed on trusted websites), how do you know which sites you can trust? Forget individual patches. Focus on updating to the latest versions of your browser. Following this, test your browser's configuration for weakness.

8. Secure your operating system

Because older operating systems like Windows XP are no longer being updated, it is easy to break into them. Make sure you are using current operating systems to take advantage of significant security improvements.

9. Secure your router

A router connects your network and computers to the Internet. Ensure that someone cannot intercept all the data sent through it. It is vital to set a strong admin password on your router and a more secure WPA2 password on your Wi-Fi connection.

10. Secure your data

If you lose data to an accident or attack, you will always be glad to have a backup. Your backups should be encrypted and stored off-site in case there is a fire or burglary.

Implementing these security steps within your organization will help make you a less attractive target to a hacker. You should also consider purchasing a Data Breach and Network Security insurance policy that will provide you with protection if a hacker is successful in stealing your data.

Steve Anderson is an authority on insurance technology. He is a prolific writer and frequent speaker known for his knack for translating "geek speak" into easily understood

concepts. Check out his free weekly newsletter “TechTips” and other resources on his website.