CYBERRISKS+LIABILITIES

May/June 2018

IN THIS ISSUE

hierl

AGGRESSIVE FOREIGN CAMPAIGN TARGETING MILLIONS OF DEVICES

The U.S. and U.K. have issued a joint warning about an aggressive campaign by Russian cyber criminals targeting internet devices in homes, businesses and government locations. According to the report, the goal of the cyber criminals is to control the devices for espionage, theft of intellectual property and preparation for a possible future attack against crucial infrastructure.

Specifically, U.S. and U.K. officials are worried about increasingly common devices in homes and businesses enabled by Wi-Fi, known as "internet of things" devices. Lax security makes millions of both domestic and commercial machines vulnerable, as they could be used not only for spying but also as tools for further attacks.

The "Mirai botnet" attack in 2016 is a prime example of the type of attack U.S. and U.K. officials are concerned about. Cyber criminals hacked into and hijacked thousands of internet-connected devices like cameras and DVRs, and then used them to ping web addresses, sending high volumes of web traffic to target servers. The resulting cyber attack was the largest of its kind ever recorded and crippled the online presence of the world's largest companies.

The U.S. and U.K. are worried that the next version of the Mirai attack could target even more devices without their owners ever knowing, especially as the number of internet-connected smart devices grows in homes and workplaces. The fear is that hackers could cause damage to more than just the devices—they could target an electrical grid or other crucial infrastructure.

Although threats from Russia are no surprise to the U.S. and U.K., the latest warning is an attempt to deter future attacks by calling attention to existing vulnerabilities and encouraging citizens to take preventive measures.

Regardless of where cyber threats originate, they are complex in nature and not expected to go away any time soon. However, the solution could be as easy as occasionally changing the default password on a home router or following recommended cyber security guidelines in the workplace.

3 Ways to Drive Sales with Cyber Security

When it comes to cyber security, it is easy for business owners to get frustrated with the efforts of being constantly on guard, as well as the extra expenses involved with it. However, instead of seeing cyber security as an expense, it may help to see it as an investment and a way to set yourself apart from competitors.

How to Make Cyber Security Profitable

When cyber security is at its best, it should improve a company's market access, branding and reputation. Although it may take a while, proper cyber security techniques should also increase revenue. Making cyber security an investment as opposed to an expense involves doing the following:

1. **Including the security team on sales decisions**—For example, if the sales team wants to target customers in highly regulated areas like government or health care, the security team should be able to assess its readiness for entering those markets. If it can't demonstrate compliance with market regulations, business owners should see that as a warning to avoid those markets, thus avoiding potential losses.
2. **Performing a risk assessment and acquiring adequate cyber coverage**—A risk assessment can help determine what type of cyber coverage is right for your business, as it identifies potential losses that could result from security failures.
3. **Realizing the damage a cyber threat can pose**—According to cyber security company Kaspersky Lab, close to 200,000 new malware samples appear daily. However, most small and medium-sized U.S. businesses assume they will not be victims. Early adopters who address their cyber security concerns can grow profitable by uncovering customer needs, easing fears, and addressing the concerns and requirements of end users.

Choosing the Right Type of Cyber Testing for Your Business

Taking the initiative to invest in cyber security and improve employee security awareness is vital for defending a business from cyber attacks. However, it may be necessary for businesses to re-evaluate their efforts on occasion to make sure their security measures are effective. Vulnerability scans, penetration testing and red team exercises are three types of tests that businesses can use to assess their cyber security.

Vulnerability Scans

Vulnerability scans and assessments use automated tools to identify cyber weaknesses. They're typically used to find known or common vulnerabilities, such as those used in past breaches and those that provide paths of least resistance for attackers trying to enter the network. Vulnerability scans are most useful for small and mid-sized organizations with limited cyber security resources.

Penetration Tests

Penetration tests are simulated attacks that use information acquired from vulnerability scans in an effort to access or penetrate the enterprise network. When a penetration test occurs, enterprises and security professionals may or may not know of the test in advance. Penetration tests can be performed by internal staff or external vendors. They're most beneficial for organizations of medium maturity looking to uncover gaps in security.

Red Team Exercises

When using a red team to assess security, employees assume the exercise is a real-life situation and do not know about it in advance. Red team exercises help organizations gauge realistic responses to attempted attacks by mimicking attackers and attempting to break into the organization in any way possible. Mature organizations with specialized cyber security skills would benefit most from red teaming exercises, which can uncover security gaps both inside and outside of the network. Red team exercises can be conducted by internal staff or by external vendors.

Once an organization identifies which type of testing is appropriate, it should also assess the frequency of the testing. Ultimately, every new or updated technology should be subjected to thorough testing to detect and address new vulnerabilities before outside attackers find them.

This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.