CYBERRISKS+LIABILITIES

IN THIS ISSUE

JRG ADVISORS

88 Percent of Employees Lack Knowledge to Prevent Cyber Incidents

According to a recent report, 88 percent of employees lack the understanding necessary to prevent common cyber incidents.

That report is based on the results of a survey given to more than 1,000 employees across the Unites States, and was designed to test the level of knowledge and awareness of cyber security among employees by asking them to name proper behaviors in given circumstances. The survey covered eight risk domains and assigned three risk profiles—Risk, Novice and Hero—to indicate an employee's privacy and security awareness level.

Key findings from the report include the following:

- Only 12 percent of respondents earned a "Hero" profile, while 72 percent were given a "Novice" profile and 16 percent were given a "Risk" profile.
- Almost 40 percent of respondents disposed of a password hint using unsecure means.
- About 25 percent of respondents failed to recognize a sample phishing email, even though it came from a questionable sender and included an attachment.

Educating Employees

This report highlights one of the key vulnerabilities of any organization—employees' lack of basic cyber security knowledge. Regardless of other hardware or network protections, employees can and will allow cyber criminals into an organization, often without even realizing it.

Fortunately, employee cyber training can help reduce this risk to your organization. For employee cyber training resources, contact JRG Advisors, LLC today and ask about our Employee Cyber Training Manual.

Despite Fears, U.S. Officials Saw No Reports of Cyber Attacks on Election Day

Despite widespread fears from cyber security experts and widespread distrust of the integrity of the voting system on the part of the electorate, the U.S. Department of Homeland Security (DHS) said that there has been no evidence of any cyber attack disrupting voting on Election Day.

After an election season filled with data breaches, leaked documents, and allegations of both election fraud and state-sponsored cyber crime, many were fearful that a cyber attack could disrupt polling. Roughly 1 in 6 voters said they were not confident that their vote would be accurately counted, according to some exit polls. However, DHS has found no evidence of any such attack, despite closely monitoring the situation on Election Day.

It's possible that increased cyber security deterred cyber attacks. Given the increased concern, DHS offered its services to any state concerned about possible cyber threats on Election Day. All but two states accepted help from DHS in monitoring their states' voter registration and election systems for potential threats.

NHTSA Outlines Best Practices for Cyber Security in Vehicles

The National Highway Traffic Safety Administration (NHTSA) has released guidelines for cyber security in vehicles, designed to give vehicle manufacturers best practices to abide by as cars become a larger target for cyber attacks. The document provides non-binding guidance, meaning that there is currently no regulatory standard that carmakers must abide by. Rather, the NHTSA hopes that by offering these standards, carmakers will be able to reduce the chances of cyber attacks committed against vehicles they manufacture.

Among the highlights of the guidelines are a layered approached to cyber security—one that would prioritize the safety of critical systems over incidental systems—and the sharing of data with other carmakers as well as the NHTSA.

Criminals Hijacked 100,000 Devices in Dyn Cyber Attack

Dynamic Network Services Inc. (Dyn) said that more than 100,000 devices may have been involved in the massive cyber attack that overwhelmed its servers and produced a ripple effect that temporarily shut down access to sites like Twitter and Netflix for much of the northeastern United States in October.

How the Attack Worked

This cyber attack was what is known as a distributed denial of service (DDoS) attack. A DDoS is a type of cyber attack that hijacks multiple devices—usually through installing and spreading malware—to "flood" a specific group of servers with a multitude of requests for information all at the same time. The tactic effectively "clogs" the servers so that they're unable to handle normal web traffic and can ultimately force them to shut down temporarily.

In the past, attacks like these would typically utilize personal computers to carry out the attack. In this case, however, it appears that the attack co-opted a number of "smart" devices—things like digital video recorders (DVRs), printers and even cellphones. Government officials currently believe that a non-state actor is behind the attack, but as the investigation is still ongoing, they have yet to definitively rule anything out.

Key Takeaways

Regardless of the source, the attack highlights a pair of troubling trends. First, this DDoS attack was one of a growing number of more sophisticated attacks. And, while Dyn—a company with robust cyber security measures—was able to restore its regular operations fairly quickly, it only did so after defeating two separate waves of the attack.

Second, and perhaps more importantly, this attack shows the potential vulnerability posed by the increasing number of interconnected, internet-enabled devices commonly called the Internet of Things (IoT). The interconnectivity of devices on the IoT is the source of a number of benefits; however, that very same interconnectivity offers cyber criminals an often overlooked—and potentially less secure—avenue of attack.

For more resources on bolstering your business's cyber security, contact JRG Advisors, LLC today.

JRG Advisors, LLC
7000 Stonewood Drive, Suite 251
Wexford, PA 15090
412-456-7000
http://www.jrgadvisors.net/