Cybersecurity ALERT

Follow us on

October 2016

The Internet of Things and Your Security

By Peter Schablik, CISA, CPA, MBA | Partner

This article provides an overview of the widespread Internet outage that occurred on October 20, 2016, examining the purpose and vulnerability of various Internet devices.

What Happened

On Friday, October 20, 2016, many businesses and personal IOT devices were compromised and used to perform a distributed denial-of-service (DDoS) attack on the service Dyn, which supports several popular Internet services including Netflix, PayPal, and Twitter. Hackers loaded programs onto various unprotected IOT devices that created millions of requests for services, causing an overload and interruption of service. Imagine one hundred million requests to sign up for new memberships with Netflix or to watch a streaming video on Twitter. These services were not designed to sustain this high level of volume and consequently were unable to serve, valid customers.

IOT devices connected to food service equipment are considered computers. They may not have a keyboard or be used for inventory or general ledger transactions but there is a microprocessor, operating system, memory among other components and they are susceptible to cyber-attacks. These devices are typically not afforded the same level of security scrutiny as other computers but are no less vulnerable. Another concern is that many of these devices may already have Trojan horses, or program designed to breach security, which can be activated at any time.

Why Does This Matter?
The compromise of IOT devices will likely lead to the failure of food service equipment (e.g. freezer shutdowns) or unauthorized access to confidential information. There has been some discussion regarding legal liability for the recent computer service outage. If there is an attack on an Internet service from an alarm controller in a warehouse resulting in a financial loss; who is liable? There is some concern that a court of law might consider negligence or gross negligence as a contributing factor to financial loss in this type of failure to appropriately secure devices. There is also the risk of reputation damage. Do you want your customers to know that the systems that protect their food quality are vulnerable?

What Preventative Measures Should Be Taken?
1. **Inventory Devices** - The first step is to identify potential IOT devices that are at risk. Mobile devices such as bar code readers and tablets should be included in this inventory. A review of contracts and some network scanning may also be required to identify all compromised devices.

> "The compromise of IOT devices will likely lead to the failure of food service equipment (e.g. freezer shutdowns) or unauthorized access to confidential information."

2. **Perform Basic Security Measures** – Depending upon your agreement with the vendor; you may have certain responsibilities including changing account passwords, periodically updating patches, and anti-virus, and malware monitoring. If the supplier is responsible for performing these services how do you know their effort is sufficient? You might want to consider reviewing their contracts, history of security breaches, and monitoring controls. In addition, major food service vendors may have security examination reports such as the AICPA SOC 2.

3. **Conduct a Device Penetration Test** – Similar to a network penetration test; a device penetration test may be warranted. This test probes devices for open ports, outdated patches, and permanent weaknesses such as zero-day events where no patch exists. Weaknesses, where there is a fix should be corrected, and other vulnerabilities should be regularly monitored.

4. **Continuous Monitoring** – Monitoring devices is critical. If the vendor provides monitoring, a discussion of the procedures performed is necessary. If the vendor is not performing monitoring the procedures such as changing administrative account passwords, ongoing file integrity monitoring, and other techniques should be considered. For devices connected to your internal network (e.g. alarm system controlled from network), the same procedures for protecting workstations and other internal devices should be followed.

For more information contact:

Peter Schablik, CISA, CPA, MBA | Partner
617.501.4195
Peter.Schablik@WeiserMazars.com

Visit us on **www.weisermazars.com**