The Evolving Internet of Things and Its Risks for Business Consumers

By: Kevin D. Pomfret

11.18.2016

The recent distributed denial of service (?DDOS?) attack on domain name service provider Dyn is likely to result in greater scrutiny by regulators and lawmakers of the potential risks associated with the increasing use of the Internet of Things (?IoT?). The IoT, a general term used to describe physical objects that connect to the internet, servers or other computing capability, is one of the fastest growing areas of technological advancement around the globe. Current examples include fitness trackers; smart home appliances, such as thermostats and televisions; and internet-connected cars. Businesses in a variety of industries also use IoT for tasks such as security monitoring, supply-chain management, and improving utilization of resources. For example, Rolls Royce aircraft engines send real-time data to monitoring stations on the ground, and John Deere has added connectivity to their farming equipment that helps farmers assess what, how and when to plant their crops. In the DDOS attack, hackers were able to essentially hijack IoT devices, including DVRs and webcams, and use them to flood Dyn with illegitimate web traffic. Given the importance of Dyn to the internet, the attack resulted in consumers not being able to access popular websites and services, including Netflix, Twitter, and Amazon. It is believed that hackers were able to compromise the devices due to insufficient security measures, including failure by consumers to change passwords from the manufacturer?s settings.

This recent attack highlights that, while there are undeniable advantages for consumers and business to using internet connected devices, there are also several risks. These risks generally can be divided and grouped into two large categories. First, the IoT collects a deluge of information, some of which could be considered personal information. It is therefore essential for businesses that use IoT devices to understand exactly what information is being collected, how it is being used and who has access to it. Second, the IoT is a network; it connects devices to one another. As the Dyn DDOS attack shows, the more devices that are connected to the network, the more vulnerable the network is to being hacked. As a result, a point of vulnerability in a single device that is networked compromises the security of the entire network. Developers of IoT devices are aware of these risks and are increasingly taking measures to protect against them. However, it is also necessary for businesses to understand the risks to their employees and customers and implement appropriate security.

In an effort to better understand the security risks associated with IoT, earlier this year the National Telecommunications & Information Administration (?NTIA?) within the Department of Commerce published a request for comments on the ?Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.? NTIA received over 130 responses which it is currently in the process of analyzing. Respondents ranged from software and development companies and trade groups to watchdog organizations and other government agencies.

The final guidance published by the NTIA for IoT developers and users will be based not only upon the comments it receives but also upon lessons learned from this recent DDOS attack. However, in the meantime, businesses that use or wish to integrate IoT into their operations should consider employing the following best practices:

1. **Be mindful of the default security settings.** The default setting is not always the most secure setting, so users may need to update devices? security settings manually for greater protection. In addition, manufacturer preset passwords should be changed and updated periodically.
2. **Maintain the software.** It is critical to download software updates and patches; the updates and patches are designed to preserve the devices? integrity and security as well as fix any bugs the developers have discovered.
3. **Monitor network security.** Use virus scanning software and other malware detection tools to respond to and prevent potential network threats.
4. **Employ low cost security solutions**. Using firewalls and storing data in an encrypted or other unreadable format are low cost ways to minimize readily accessible personal information.
5. **Audit data assets.** Every business is now collecting and using vast amounts of data on its customers, partners, employees and processes. Companies with large data stores are ripe targets. However, many businesses do not understand what information they collect, where it is stored, who has access to it and how long it is retained. As a result, businesses should conduct an audit of their data assets in order to limit the amount and type of data collected and retained, and dispose of the data when it is no longer needed.

Unfortunately, in this age of increasing interconnectivity, there is no foolproof way to prevent privacy and security breaches. However, employing these basic practices can help businesses create a foundation to minimize the risk of breaches as they begin to realize the enormous benefit of the IoT.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity