Security concerns rising for Internet of Things devices

Call it the Attack Vector of Things

By John Brandon | Follow
CSO | Jun 1, 2016 5:00 AM PT

The burgeoning market for gadgets that trigger a sprinkler system, help you count the number of times you swing a bat, or dim the lights automatically are rising.

That's a concern for any business due to how these devices are also starting to show up at the corporate office for use in conference rooms, executive suites, and even as a low-cost building security camera system. Experts claim the industry is not doing enough to protect these devices.

Craig Young, a cybersecurity researcher at Tripwire, says a big part of the problem is that the firmware is not updated on a regular basis.

In one recent example, researchers at the University of Michigan found they were able to hack into the Samsung SmartThings platform and even control an entire home automation system. The researchers were able to eavesdrop on the PIN code used for a new install.

"These companies sometimes have the intention of fixing a vulnerability like that through a firmware upgrade, but then never get around to it because they don't want to disrupt the user base," explained Young.

MORE ON CSO:Mobile Security Survival Guide

He described how, in some cases, he tests out a new device from a company like Belkin or Wink, finds a potential security flaw, notifies them and waits patiently to see when the new vulnerability will be patched, which can take way too long.

Young says the most common hack is to break into a connected home hub, which then provides access to any of the connected devices including door locks, motion detectors, sprinkler systems, and even the alarm system protecting a home.

Surprisingly, there are few security apps available that can monitor Internet of Things devices, let you know about any new emerging attack vectors, and tell you about any recent compromises.

"When we look at our workspaces today there are already a number of wireless devices, from Bluetooth mice to wireless keyboards, and we have very little knowledge of who develops the firmware that runs on them or where is it coming from," says Roman Foeckl, the CEO of CoSoSys.

"With the little security that is in place today for Internet-connected devices, threats will continue to multiply as more and more IoT devices are adopted, both at home and in the workplace."

Why is this a problem?

Hackers always seem to flock to the most popular platforms. It's one of the reasons there are more risks for Windows users than the Mac -- there's a much bigger footprint. According to BI Intelligence,

there will be 34 billion connected devices in the world by 2020, creating a $6 trillion industry; surprisingly, BI names business as the main IoT adopter. The costs are low, the gadgets are simple to install, and they solve nagging problems (e.g., installing a motion detector to find out how many people use a conference room during the day).

One good example of this is the Belkin WeMo platform. Young says you can install a device like this outlet that you can control with your smartphone in five minutes. Yet, there might not be any intrusion detection for a product like that. In a worst case scenario, he says, a Chinese hacker could find a vulnerability for these outlets and then power cycle them repeatedly for thousands of users all over the U.S. to cause massive blackouts. Yet, for the end-user, there is some incredible usefulness, energy savings, low costs, and a simple install.

Foeckl says it's this emerging utility and usefulness that makes IoT more vulnerable. A new connected device solves a problem, but we don't always know that much about the firmware or the software used to solve a new problem. IoT devices are ultra-simple but they often share their Wi-Fi credentials. Indeed, Young says one of the biggest risks is that hackers can intercept the password for a Wi-Fi network, which is what happened two years ago when researchers found the LIFX connected light-bulb exposed network configurations.

When asked for a statement, a LIFX spokesperson said the company takes security seriously, and has "worked hard to provide an experience that puts the safety and security of consumers, their homes, and Wi-Fi networks first. We will continue to build products that aid in the security and protection of consumer homes."

[ALSO ON CSO: The CSO IoT Survival Guide]

Craig Spiezle, who is the executive director and president of the non-profit online security and privacy watchdog group the Online Trust Alliance (OTA), says there are several problems with IoT that have made it such a large attack surface.

For starters, consumers and businesses are starting to depend on these gadgets; the adoption is fast and furious, which means security is a secondary concern. There isn't the same robust security testing and patch management given to other, more mature products like servers and smartphones.

Another issue he mentioned is that there might be an effort with IoT devices initially, when the product is new, but there are too many "orphaned" devices still connected to networks that are left unpatched and ignored. A prime example of this is the Nest Revolv smart hub. Researchers found serious security flaws, in April Nest announced the company would discontinue the product and would not update any of the firmware.

Young says an even more critical problem is that many of the smaller IoT companies have a small staff -- they do not even have security professionals working for them, and they tend to use third-party electronics that may or may not have been certified or even tested for security. The market is so new, the main goal for now is to get these gadgets to market quickly.

What can be done?

The good news is that the larger IoT companies like Belkin are starting to respond to the problem. Young says he has seen progress in how often companies are responding to firmware problems or at least acknowledging that there is a growing problem. Indeed, when LIFX found out about the Wi-Fi

credentials flaw, they patched it right away.

Because there are so many small companies making IoT devices, the problem won't go away anytime soon. Foeckl says IT departments need to start including IoT devices in their security monitoring efforts and certification and testing processes, and that they should work with their vendors to make sure these devices are patched, tracked, and protected.

"Another important task is the development of privacy policies that inform users about the collected information and guide them to maintain a security good practice, advising on changing passwords, reporting unusual activity," says Foeckl. "A well informed user represents a great premise to prevent data breaches regardless of the threat vector."

Spiezle says one answer is to develop a comprehensive IoT device certification program such as OTA's Trust Framework as a way to combat the free-for-all. Intel has also stepped up to the plate and has made security for IoT devices a bigger priority.

Ultimately, the real answer has to do with IT purchasing decisions. Dan Lyon, the principal consultant at security-as-a-service firm Cigital, says businesses need to start evaluating IoT products not only for the benefit they provide but also for embedded security features.

"Once the risks are understood, the business can start requiring the manufacturer make the systems secure and to support them in the long term." he says. "When these aspects are used as a purchasing decision point, then the manufacturers will respond appropriately."

That might not solve the problem with legacy IoT devices, and could even slow market adoption, but businesses (and consumers) might be able to breathe a little easier.

[*Samsung responded to questions related to this article by directing CSO Online to their previously issued statements, which can be viewed on their blog.*

Wink said they work with both internal and external security experts to "ensure security standards are exceeded" in addition to regular audits by third-party researchers.

"Transparency is key, and to that end, we've previously collaborated with BugCrowd on a bug bounty program for all Wink products."

When asked for more information about how they're addressing IoT vulnerabilities, Belkin did not respond to requests.]

John Brandon — *Freelance Writer*

John Brandon is a respected technologist, product tester, car enthusiast, and professional writer. Before becoming a writer, he worked in the corporate sector for 10 years.