BTB SECURITY

ARE IOT DEVICES COMPROMISING YOUR SECURITY?

AS MORE DEVICES BECOME INTERNET-ENABLED, THE ALREADY-NUMEROUS WAYS HACKERS CAN GET INTO YOUR NETWORKS ARE SKYROCKETING.

Gartner expects 20 billion Internet-connected things to be online by next year. In many cases, these devices are akin to hanging out an "enter here" sign for the bad guys.

Kaspersky Labs has seen a three-fold increase in the number of malware variations used to attack IoT devices, according to the company. A recent CapGemini study reported that cybersecurity incidents through IoT devices are up 16 percent. Security cameras are a common culprit, but as more things - phones, lights, thermostats, and yes, even toasters – are connected, the attack vectors are exploding.

Unlike computer hardware and software suppliers, companies that sell devices like cameras, lighting and other facilities equipment don't always consider IT security. Their designers likely do not have IT backgrounds, much less cybersecurity backgrounds. Their priorities are more likely to be ease of installation and ruggedization against the elements than ensuring against hacking.

Until recently, buyers haven't thought much about security either. But the government has started to. California just passed the nation's first IoT security law. Scheduled to go into effect on January 1, 2020, the law requires IoT devices sold in California to be equipped with reasonable security measures. Meanwhile, a bill introduced in the U.S. Congress calls on the federal government to study IoT security.

Although awareness is increasing, "there remains a level of perceived security through obscurity," says Matt Wilson, BTB's Chief Information Security Advisor. "Companies think that hackers won't know about the internet-connected devices, so there's little danger." That's a dangerously incorrect assumption. "Just because you can't envision a way doesn't mean that attackers can't," he says. "This is a very real risk that companies need to assess and address."

ASSESS AND ADDRESS

HERE'S HOW:

- **Identify all internet-connected devices in your company.** "You can't protect what you don't know about," says Wilson. This identification step may not be so easy, especially if policies have not been updated to cover IoT devices. What if your facilities manager decides to install smart lighting or a new badge-access system? Has your HVAC vendor upgraded your system with a smart thermostat? Maybe one of your employees thought it was a good idea to install a smart speaker in the break room.

- **Update your procurement policies and supporting processes so that you (and your IT department) will know when such devices are brought into your facility,** and that your standard security policies and practices are applied to them. Make sure people in all departments of your company, including facilities operations, logistics and end users themselves, are not only aware of these policies but understand their significance and potential impact to the organization.

- **Know how the devices connect to your system, both logically and physically.** What wireless protocols do they use? What hubs do they connect to? If and how they communicate externally.

- **Determine whether the devices store data and, if so, identify what kinds of data.** Is any of it personally identifiable information? Does it include internal credentials, such as user names and passwords, that a hacker might leverage to gain access to other parts of your network?

- **Know how the devices connect to your system, both logically and physically.** What wireless protocols do they use? What hubs do they connect to? If and how they communicate externally.

- **Who in your organization is responsible for the operation and maintenance of the devices?** Are they taking the right precautions? A facilities manager might be used to thinking about physical security, but overlook the fact that a hacker could break into an internet-connected badge access system and steal credentials that would let him impersonate an employee and walk right in to the most sensitive areas of your business. The transportation department might like having GPS on all its vehicles but be unaware of the possibility they could be hijacked. "IoT takes the problem of asset management that everyone struggles with already, and just exponentially detonates it," says Wilson.

- **Segment your network based on risk profile, keeping many of the IoT devices on a network that is separate from your most important data and operations.** "Consider what could be damaged if this particular thing got hacked," says Wilson.

HOW TO MITIGATE IOT DEVICE RISKS

The U.S. National Institute of Standards and Technology just published a draft guide about the risks of IoT devices, and how to mitigate them[1].

RECOMMENDED SECURITY FEATURES FOR INTERNET-CONNECTED DEVICES:

- An ability for the device to identify itself on the network
- Capability for an authorized user to access and change the device's configuration
- Clarity on how the device protects data from unauthorized access
- Limits on the access to the devices' logical and network interfaces
- Updatable software and firmware
- A capability to log cyber security events and make the logs accessible

[1] https://www.nist.gov/news-events/news/2019/06/connecting-iot-device-check-out-new-nist-report-cybersecurity-advice

GET AHEAD OF IOT RISK

NIST is gathering feedback on the draft and plans to update it. Nevertheless, the document is a good foundation for IoT security, says Wilson.

Get ahead of IoT risk by securing your business now. Develop policies and processes to identify what IoT devices are coming into your organization and to ensure that they are secured. And, as more and more things become internet-enabled, schedule routine assessments to spot whether any new devices have snuck in or whether previously unconnected devices are now on your network.

FOR MORE INFORMATION ABOUT HOW YOU CAN IMPROVE YOUR ORGANIZATION'S SECURITY POSTURE VISIT WWW.BTBSECURITY.COM

ABOUT THE AUTHOR

Matthew Wilson is an Information Security Advisor at BTB Security, a specialized cyber security services firm that specializes in proactively detecting threats as well as defending against and defeating cyber security adversaries. His background in network security, penetration testing, and assessment helps organizations shield their assets, customers, and employees against security breaches.

MATT WILSON
(CISSP, GPEN, GSEC)

WHAT WE DO

BTB Security helps organizations worldwide detect, defend and defeat security breaches. From ethical hacking and vulnerability assessments to comprehensive managed security services programs, incident response and forensic analysis, BTB's solutions are designed to provide comprehensive security to organizations of all sizes.

BTB SECURITY