The Internet of Things

SecurIT360
The physics of securing IT

So, what exactly is the "Internet of Things?"

The Google definition states that the internet of things is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

In other words, any device connected to the internet, which has memory, a processor, and the ability to send and/or receive information.

That still sounds like an IT network, but it is much more. Think of any device that can be connected to the internet via a wired network, Wi-Fi network, or cellular network. Think of anything at your home that can be controlled by a cellphone app.

For example –

- Smart Home Apps, which control -
  - Thermostats
  - Lights
- Security systems
  - Door and window locks
  - Cameras
  - Spotlights
  - Alarms
- Baby Monitors
- Smart Appliances
- Stereo Systems
- Home Wi-Fi
- Wearables
  - Fitbit
  - Apple Watch
- Amazon Echo
- TV Remote App

Now, extend that thought to business tools (outside of your traditional IT network) which may also be connected to the internet. Here are a few examples.

- Connected vehicles
- Medical devices (including pacemakers)
- Fuel Control Systems
- RFID Systems
- Robotics
- Building Controls
  - HVAC
  - Access controls (card readers and door locks)
  - Fire suppression systems

While they have been around a long time and were originally on analog networks, SCADA systems are certainly part of the Internet of Things.

It is always critical to remember that anything connected to the internet has the potential to be "hacked" and controlled by someone else. That is why it is so important to know and identify every single device in your business (or home) that is connected to the internet. We must apply sound cybersecurity rules and controls to IoT devices.

The FBI has published a PSA regarding the IoT. https://www.ic3.gov/media/2015/150910.aspx

dburns@securit360.com

The Internet of Things

SecurIT360
The physics of securing IT

What are the dangers of the Internet of Things?

Any device or system which can be hacked, can also be disabled, destroyed or misused.

Imagine the consequences of any of the devices / systems listed above in the following conditions.

- Unable to turn On or Off
- Inaccurate information or readings
- Settings too high or too low
- Device or system disabled

However, the individual "owning" of devices or systems is not the only danger. When IoT devices are controlled in mass, that provides an exponential power factor to affect damage on a much larger scale.

This was proven recently by the Denial of Service attack on the Internet provider, Dyn.

The Marai botnet was used to infect and control millions of IoT devices, such as, printers, baby monitors, IP cameras and residential gateways. These devices were programmed to send malicious connection requests to the Dyn systems at precisely the same time, flooding their system with so much traffic, that they were rendered virtually useless.

Some of the end user companies affected by this include –

- Amazon
- Comcast
- Fox News
- CNN
- New York Times
- PayPal
- Pinterest
- Starbucks
- Twitter
- Verizon
- Walgreens

Some basic rules for IoT devices

- Inventory all devices and systems
- Do not use default passwords
- Segment to separate networks where possible
- Be sure that software is always up to date.
- Do not connect it to the internet until all security tools are in place.
- Conduct a 3rd party assessment of all connected devices and policies

You may not be able to completely secure every device, but don't make it easy for the bad guys.

As always, develop a "cyber-defense" mindset to protect yourself AND your company.

If you would like to learn more about Cybersecurity and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250