IoT: The dangers and technical security challenges for the Internet of Things

By: Brad Voris

IoT devices are a nightmare for Information Security Professionals, System and Network Engineering Professionals. But why? What is the "Internet of Things"? How has IoT started to change the face of business?

The Internet of Things (IoT) is a term to loosely describe "smart" devices that connect to the internet or a network to transmit or receive data. A few examples of these devices are: smart watches, multimedia streaming devices, biometric sensors, remote seismic sensors, home automation and monitoring devices. These IoT devices can do many things from collecting audit data, generating reports, streaming multimedia to providing content across networks. The possibilities for data collection are practically endless.

Is your business or personal information being sent from the IoT device out to vendors, manufacturers and/or marking companies? Are your business audit logs being sent directly to your IT department or is there a third party involved? Are those cameras you have recording your business sending snapshots or streams to the cloud? Who is managing this data? Is this data being encrypted during transport and while being stored? Is that smartwatch connected to your wireless network transmitting your personal information to the internet? Does this data publically expose private personal or business information?

There is massive financial gain from PII (Personable Identifiable Information), PHI (Private Health Information), and insider business information that should be confidential. This kind of information is bought and sold on the *Darknet* along with credit card numbers, social security numbers and passports. Vendors can sell this information to marketing companies to use for targeted advertisements.

This is the kind of data you don't want exposed.

I.E.: If said IoT device is monitoring temperatures in your home or business, it could send statistical data to the manufacturer or vendors for maintenance or parts.

Hackers could intercept and use this data to gain more information about an individual or business using this knowledge against them (social engineering or physical security break-ins).

How secure are these IoT devices?

I can't speak for every IoT device only the ones I have worked on. Most IoT devices out of the box have simple passwords or minimal security. Some of these IoT devices have hidden backdoors, software maintenance hooks, and phone home. Very few use any kind of encryption or integrate into any kind of identity access management system.

How do I secure these IoT devices in my environment?

Baseline. Start a baseline for devices in a test environment. Not all IoT devices are bad, but know the dangers of putting an IoT device on your network that someone could potentially gain access to or could provide transparency on your private information.

Things you can do to protect your network and systems from potential attacks:

1) Create policies and standards for IoT devices in your business.
2) Disable default pre-configured accounts (guest, admin etc.).
3) Change root, admin, administrator, guest passwords.
4) Get the latest firmware / OS update for these IoT devices prior to deployment in your environment.
5) Monitor traffic by using a packet sniffer to see who and where the IoT device is communicating with.
6) Configure firewall rules to prevent traffic to and from these IoT devices, or only as necessary (maintenance window).
7) Segregate traffic to a separate VLAN, network or on the DMZ – if the IoT device doesn't need direct access to your network put it someplace else. (Guest wireless network access).
8) Encrypt data if at all possible.
9) Product lifecycle – determine a product lifecycle before implementation; this should include planning, deployment, administration, updates, upgrades, and retirement of the IoT device.

Does the IoT device provide a static service that doesn't need access to the internet or doesn't need to be updated regularly?

1) Change the default gateway to 127.0.0.1 (127.0.0.1 is the local loopback address; this prevents connectivity to the internet and loops traffic back to the IoT device itself.)
2) Change DNS to 127.0.0.1
3) Block inbound and/or outbound traffic to the internet through a firewall
4) Only allow traffic from specific IP addresses and ports to access the IoT device

Keep in mind that the IoT device should have a maintenance lifecycle where it is still updated appropriately. This maintenance lifecycle should include from inception to retirement of the product not just implementation and administration.

There are massive benefits to some of these devices however they need to be monitored and secured as best as possible to mitigate any potential risk involved.

Security is everyone's responsibility and the key to mitigating potential risks.