Guidepost

PRACTICAL TIPS FOR IOT SECURITY – A READINESS REFRESHER GUIDE

The Internet-of-Things (IoT) revolution has certainly taken the "cyberspace" by storm. Newly manufactured devices today must be network-ready (hardwired and wireless, to include Bluetooth, RFID, etc.). This explosion of IoT devices has presented a "nervous" feeling concerning InfoSec, compliance and privacy within companies as well as consumers who want to use these products confidently and ensure that they will not introduce any new or expanded attack surface for malicious threats targeting their network(s) and critical information. What can be done in short order to address the risks?

Below are a few recommendations to help your IoT implementations become more risk-acceptable:

1. Understand the IoT device manufacturer's approach to security. When purchasing IoT devices, make sure the sales or manufacturer representative can clearly outline the security precautions and disciplines they have used in creating the overall product. Conducting independent research regarding specific IoT vulnerabilities is well worth the effort as well.

2. Plan and design for resilience. If possible, make sure you segment your network by placing similar IoT devices in their own individual partition of your overall network. This will minimize downtime (due to software/firmware updates, maintenance, etc.) of your core business network as well as provide some level of resilience in case one of these devices becomes infected.

3. Get your "lists" together. You should have a listing of all your IoT devices and their associated technical DNA, such as IP addresses, Mac addresses, Operating System/Firmware versions, ports open/closed and services enabled at a minimum. As many (if not all) cyber experts have said, "getting breached is not a matter of if, but when…" Having up-to-date lists will allow you or your Incident Response Team, to triage, quarantine and resolve any breach-oriented issue that might arise.

4. Alert on meaningful events. One of the greatest security benefits of including IoT devices within a company's environment is that it can give you more information (if configured properly) regarding potential breaches that might be occurring deeper within a company's systems. This additional information can significantly increase your ability to visualize "actual" risk more clearly by combining IoT events with other infrastructure events.

Integrating multiple types of IoT devices does not need to be an unpleasant exercise. With practical and forward-looking measures, you can position your network environment and business to be resilient to threats from IoT, while having a robust defensive and sustainable security posture.

Key points to remember:

- A proactive cyber mitigation plan will assist greatly in remediating IoT threats.
- More up-front data equals less downstream exposure.
- Layers of resilience will decrease downtime or breach potential.
- Have your work flows pre-positioned prior to an incident.
- Anticipate potential alerts before they occur.