RSA® Conference 2019

BETTER.

Peer2Peer

Best Practices for Securing Enterprise IoT

P2P2-W15: Best Practices for Securing Enterprise IoT

John Johnson, Senior Advisory Manager, Industrial Cybersecurity & IoT, Deloitte & Touche, LLP

Best Practices for Securing Enterprise IoT

Every organization must face and deal with cyber risk associated with Internet of Things (IoT) devices connecting to other systems and the extended enterprise network. I had the privilege of leading a group of information security professionals in a Peer-to-Peer session at RSA Conference on March 6, 2019, and I learned that this problem is pervasive across all industries.

I started by asking for people to share their problems and concerns, with the understanding that there would be no attribution. There was a blend of commercial IoT and Industrial IoT concerns that we addressed.

Commercial IoT devices can be security cameras, facility lighting, even a Roomba (autonomous vacuum cleaner). The list of commercial IoT devices is almost limitless, and yet the consensus was that these devices really cannot be managed by central IT support teams. The other observation was that these devices are often not purchased by IT, but by a business owner who feels justified in the investment to solve some problem that either IT cannot solve, or because the purchase is expedient and solves an immediate problem. Policies that prohibit such devices may have some effect, but participants felt that more active measures to identify these devices on the network were required. Another observation was that there needs to be a process for requesting and vetting these commercial IoT devices. They may prove beneficial, but there is a definite need to assess the risk they introduce.

When we discussed Industrial IoT (IIoT), concerns shifted to embedded systems (running an operating system such as Windows, where the version is often older and with limited functionality) and industrial control systems (ICS), such as programmable logic controllers (PLCs). These non-traditional devices can include factory systems, monitoring and control for utilities, robots and more. As with commercial IoT devices, these systems most often were procured by business owners or unit IT personnel and not acquired through a central enterprise IT procurement process with risk assessment. These disparate and heterogeneous systems connected to our enterprise networks over the course of many years. Some of these systems are old and have few management capabilities. We agreed that these systems usually serve an important business purpose, but without understanding the risk they pose and interdependencies with other IT systems, and often without a complete inventory of these devices, they are difficult to manage well and impact an organization's security and resiliency.

Other topics, such as Bring Your Own Device (BYOD) and the need for special access for suppliers' remote management and support of specialized devices came up. For the most part, the consensus was that all non-standard (non-compliant devices) needed to have an onboarding process, which includes identifying:

- Device information (IP address, MAC address, machine name)
- Business Owner
- Risk Owner
- Risk Assessment (Why is it non-compliant? Can the risk be accepted or mitigated?)
- Purpose of device (software and services)
- Importance and interdependencies

- Data classification
- Support Plan – which team will support this device, or will a supplier need to provide external support services? (e.g. restricted VPN)
- Review plan – purpose and vulnerabilities may not be static (e.g. Annual compliance recertification)

The onboarding process should be developed and customized for the needs of the organization, including relevant and representative enterprise stakeholders.

Most attendees agreed that they did not have good knowledge about what is already connected to their enterprise network, so a discovery/inventory process is crucial, however this is easier said than done. While many commercial IoT systems are designed to be resistant to TCP/IP and UDP network scans, many specialty IIoT systems can be affected by running an IT discovery scan. Even something as innocuous as sending an ICMP Ping to a factory robot, could cause it to rotate or act in an unanticipated way. Yet, identification of all the non-compliant and “rogue” devices on your network is a top priority. This means that there needs to be leadership from the top-down supporting risk management on IoT systems. It will take boots on the ground to find and onboard all of the existing IoT systems, and to implement risk mitigation steps (e.g. changing default passwords) and perform regular audits and annual compliance recertification.

There was no single technology or process that proved to be a silver bullet for securing the IoT systems, once they were onboarded as managed assets. The group came up with a fairly good list of best practices, which will need to be customized. For consistency, processes that can be automated or included in standard processes are better.

- Inventory – scan or otherwise enumerate IoT and IIoT and other non-compliant devices (without disrupting them)
- Assess and manage risk (consistent with an enterprise risk management program)
    - ACL restrictions
    - Network (IP-based) restrictions (e.g. Restrict Internet Access)
    - IPv6 can introduce more security headaches and loss of visibility to incidents
    - Have a process for dealing with new network segments as they are added
    - Possibly utilize NAC if compatible
    - Group Policy restrictions and remove Local Admin Rights (e.g. No USB policy, restrict software installations)
    - Special routers, firewalls, etc. to restrict traffic and prevent dangerous commands for non-TCP/IP devices
    - Utilize traffic anomaly monitoring tools (few exist but this is a growing area)
- Training
    - IT staff may not be well-versed in operational technology (OT) with non-TCP/IP protocols
    - Train the people who will be managing and supporting these devices

The attendees agreed that this is an iterative process that needs to improve over time; you will not be perfect out of the gate. Nevertheless, it is vital to build competency and mature capabilities around the management and support of non-standard, IoT and IIoT systems and OT protocols. The other piece of advice that was offered is not to wait for a perfect inventory before moving onto other steps. Perfect is the enemy of good! The advice was to work in parallel, not a series approach. Start enumerating devices and onboarding them. At the same time, start appropriate mitigation steps, such as network segmentation, Group Policies, NAC and monitoring.

Another way to look at the basics for starting an IoT security program is: Visibility, Segmentation and Monitoring. Visibility does not mean a complete inventory, rather start with what you have and passively analyze network traffic to get a preliminary picture of the current state. This can help you prioritize the ways in which you segment and mitigate IoT cyber risk. Finally, ongoing monitoring can potentially help you understand what is normal for your IoT traffic.

After all of this, securing IoT systems is a journey, one that is highly important to the security and business continuity of your organization, so you need to start down this road today. Reach out to peers and experts for advice. Despite past lack of focus and resolve in this area, together, this is a problem we can tackle and solve. As we look to the future, there will be more automation, consumer and industrial IoT, and as IoT converges with and is enabled by other emerging technologies such as AI/Machine Learning, Edge Computing, Cloud Computing, and faster 5G networks, threats will rapidly grow and we need to be able to respond quickly and effectively. To paraphrase the theme of RSA Conference 2019, together things can only get better.