Pulse Secure®

Zero Trust and IoT

How to mitigate IoT security risk

Getting practical with IoT security

IoT adoption in the home and workplace doesn't show any sign of slowing down. Analyst firm IDC predicts that there will be 200 billion connected devices by 2020 and if standards stay the same that could mean billions of security vulnerabilities. The Marai virus demonstrated how IoT devices with default settings are vulnerable to infection and its effectiveness when used in DDOS attacks. There are more malicious variants underway that target ARC processors embedded into a broad array of Linux-based devices.

A recent survey of IT professionals found that less than half of their organizations incorporated security policies that covered IoT devices, and only a third could say it covered home networks used to access corporate systems. Knowing what devices are on your network and implementing comprehensive network access control systems are critical to staying on top of security vulnerabilities

To help mitigate these risks, this 10-point list provides some simple yet effective steps for device discovery, management, and access control that organizations should adopt across every network that either currently has, or potentially could have, IoT devices on it.

1. **Assume there are IoT devices on your network.** Regularly schedule network profiling tools to identify devices that generate anomalous responses and create device profiles that make device spoofing less likely.

2. **Prohibit or severely restrict automatic connections via WiFi or other means.** This could even go as far as network device isolation if a device only needs to talk to the local router. This helps prevent device infiltration.

3. **If incoming traffic is not blocked, check for open software ports** that allow remote control and configure or restrict access as appropriate.

4. **Research and carefully review the security characteristics and privacy policies** of the controlling apps and backend services. Do not use devices that rely on apps or services with poor security and privacy.

5. **Verify that physical access does not allow intrusion** (e.g., by factory reset, easily accessible hardware port or default password).

6. **Place IoT devices on a separate, firewalled and monitored network.** Disable or remove unused or uneeded services. This allows you to restrict incoming traffic, prevent crossover to your core network and profile traffic to identify anomalies, and reduce risk with unused or unnecessary devices and features.

7. **Deploy IoT devices within a centralized policy-based Network Access Control (NAC) platform** allowing IT managers to respond more quickly to new IoT vulnerabilities. This platform approach also makes it possible to simplify enterprise-wide deployment and rapid adoption of uniform access control policies for thousands of IoT devices.

8. **Enable encryption whenever possible** so that data is never transmitted "in the clear." Consider only buying devices that support strong encryption. Otherwise, consider using a VPN or other means to limit data exposure.

9. **Use dynamic addressing of unmanageable endpoint devices** using media access control (MAC) address authentication. This allows for the use of MAC address whitelisting and blacklisting to create resource-based access control of unmanageable devices such as networked printers, cash registers, bar code scanners, VoIP handsets, and IoT devices.

10. **Update all passwords (local and remote, if different) to strong passwords** and use multi-factor authentication wherever possible. Do not use products with hard-coded passwords. Closely govern permissions for devices, delegating access only when necessary.

This list offers a real world set of practical actions that can help reduce IoT risk vulnerability. Pulse Secure's device discovery and profiler features allow administrators to continuously run detection routines that classify managed and unmanaged devices across the network with detailed reporting to streamline management and security policy enforcement. Using this as part of Pulse Secure's Network Access Control solution provides the most efficient method of discovering, profiling, and securing every device, as everything is contained within a single GUI, enforcement and reporting structure.

Pulse Connect Secure is the most reliable and feature rich mobile VPN built for the next generation, enabling secure access from any IoT device to any enterprise app and service in the data center or cloud.

As IoT continues to spread across corporate networks, IT managers would be wise to bring these devices into the existing network access control processes instead of trying to create separate silos which ultimately lead to duplicated and unproductive workloads. It is worth making it a priority that ahead of IoT purchases, organizations mandate that each device must adhere to standards-based device monitoring and management protocols such as SNMP, UPnP, X.509 or Open Trust Protocol (OTrP) to name just a few.

Ultimately, user demands will force IoT manufacturers to offer better security capabilities which will make the IoT revolution a safer journey for enterprises and consumers alike.

About Pulse Secure

Pulse Secure, LLC offers easy, comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. Our proven platform uniquely integrates cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net

Corporate Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net