Master IoT Cyber-Security Challenges with Comprehensive, Multi-layer Security

From the smart lock on your front door to the printer down the hall, you interact with the Internet of Things (IoT) dozens of times a day. In fact, in 2019, the number of connected devices jumped to more than three times the world population. In addition to convenience, that growth has also brought significant IoT cyber-security challenges.

Unfortunately, in their rush to meet consumer demand, manufacturers have paid more attention to features than to security. At the same time, global standards have failed to keep pace with innovation. With an ever-widening attack surface and valuable data ready for the picking, cyber-criminals have stepped up their attacks.

To protect business assets and sensitive data, organizations need to better understand the IoT environment. They must keep abreast of evolving cyber-threats and develop proactive solutions for modern problems.

IoT Cyber-Security Challenges Increasing

Unlike the traditional internet, the IoT connects devices, not people. Those devices appear in every aspect of daily life, from the kitchen to the factory floor and the emergency room. With this new environment come new threats, including:

- **No centralized accountability** – Nearly every department in an organization uses IoT devices. While IT manages the network, the individual departments likely manage the devices in their area. All too often, no one takes responsibility for the overall IoT environment, and security falls through the cracks.

- **Larger attack surface** – According to a study by the McKinsey Global Institute, every second of the day, 127 new IoT devices connect to the internet. Each connected device means one more access point for hackers to attack.

- **IoT devices fly under the radar** – With so many IoT devices in use, organizations may struggle to produce a complete list of devices on the network. Monitoring those devices presents a daunting task. As a result, organizations may never know a device has been compromised.

- **Outdated hardware and software** – Device manufacturers focus more on innovation than security. And when they do produce patches to address vulnerabilities, users often fail to apply them.

- **Weak credentials open the door** – Many connected devices come installed with default usernames and passwords. Unfortunately, users often neglect to change those credentials, leaving easily-compromised passwords like "password" or "123456."

- **Viruses and malware** – A recent study conducted by Kaspersky Lab showed that malware attacks on smart devices have tripled since 2017. Infected devices include hundreds of thousands of devices from major brands.

Protect the Entire IoT Environment

The IoT ecosystem includes much more than the smart device, and each component of that environment requires protection. This includes the device itself, the software that runs it, the network it connects to and the cloud that stores the data produced.

Protecting that environment from IoT cyber-security challenges involves a multi-layer security strategy. Begin with a strong firewall and end-to-end encryption. Apply software and hardware patches quickly. Carefully define user permissions and log all system activity. Finally, regularly test the entire system for vulnerabilities.

Always Verify, Never Trust

In contrast to the old "trust, but verify" model of cyber-security, many organizations have begun to adopt a "zero trust" model. Under this model, the system verifies all connection requests before granting access.

For instance, a hacker might gain access through a connected printer and then attempt to move laterally through the system to the intended target. However, when IoT devices reside in a segmented network, it keeps infiltrators from reaching sensitive data in the main network.

Zero trust security also focuses on user identity, restricting access according to job description. Credentials for privileged users require special attention, as these are particularly attractive to hackers. As a first step, implement multi-factor identification for privileged users. In addition, monitor the system for users attempting to access areas outside of the scope of their duties.

AI and Machine Learning to the Rescue

Just as technology innovation increases the attack surface, evolving technology also provides part of the solution. Advances in artificial intelligence (AI) and machine learning allow for monitoring of the IoT landscape in ways humans cannot replicate.

For example, an AI-powered threat detection system can quickly build a profile of each user on the network. Then, when it detects unusual activity in a given user account, it alerts IT and automatically takes action to contain the threat.

Enlist Expert Help to Counter IoT Risks

With deep expertise in comprehensive security solutions, eMazzanti will help you implement solid strategies to address IoT cyber-security challenges. From implementing advanced threat protection and cloud services to securing your network, we have you covered.