IoT Cyber Security Requires a Deliberate Approach Due to Inherent Risks

Industry and individuals alike have embraced the Internet of Things (IoT). Connected devices from security cameras to complex industrial machinery gather and share immense amounts of data. But the seemingly limitless opportunities for innovation also bring significant risk. IoT cyber security best practices help companies balance risk and innovation.

IoT Brings Inherent Risks

From recent IoT cyber security news we learn that a white hat hacker used Bluetooth to hack into a Tesla Model X in under two minutes. And, hackers attacked video surveillance company Verkada, compromising 150,000 active surveillance cameras, many in secure locations.

Thus, the very nature of the IoT requires an updated approach to risks. To begin with, the IoT operates largely without human intervention. Sensors collect, share and act on data constantly, typically in the background. Data collected and shared often includes sensitive data and nontraditional data types, such as GPS location and facial recognition data.

Storing, organizing, securing, and transferring that data creates new challenges for data governance. Data enters the system in a wide variety of formats and using a variety of communication protocols.

Additionally, each device represents another possible access point for hackers, greatly broadening the attack surface. Too often, device manufacturers overlook security concerns in the development process. Indeed, many IoT devices lack the capability of supporting device security. Hackers know this, and they continually look for vulnerabilities to exploit.

Finally, the organizations and individuals that deploy IoT devices too often plug and play the devices without addressing security. They neglect to change default passwords and device names or install security updates.

IoT cyber security can prove complex. However, the following security best practices will get organizations started on the road to balancing innovation and security.

Identify Connected Devices and Update Status

First, take an inventory of devices across the IoT infrastructure. Understand what they do and identify older models that may present increased security challenges. The initial inventory process can take some time, but it allows organizations to classify devices more easily for risk management.

For each device, determine the patching status. Where possible, set devices to install security updates automatically. And when purchasing new devices, make sure the manufacturer takes security into account and provides regular updates.

Assign Unique Identities and Credentials

Devices typically come with default device names and passwords. Too often, organizations leave the default credentials in place, leaving devices and the network vulnerable to hackers. Make sure that each device and system has a distinctive identity.

Additionally, replace the default password immediately when deploying a new device. Use healthy password practices. This includes creating strong passwords, changing passwords regularly, and not reusing passwords.

Deactivate Idle Devices and Features

Each new device and each feature on the device add more access points for attackers to exploit. Conduct a regular review of devices and disable any devices or features not used regularly. Likewise, when purchasing new devices, keep security in mind. For instance, unless you need a USB port, avoid purchasing a device that includes one.

Address Physical Security of IoT Devices

Some of the most damaging attacks through the IoT involve physical access to IoT devices. Guard against such attacks by taking measures to enhance the physical security of IoT hardware. For example, securely cover USB ports. And if devices must be installed in unsupervised locations, make them as tamper-proof as possible.

Ensure Constant Monitoring

As with other facets of the system, conduct regular security audits of IoT devices and implement continuous monitoring. Network monitoring will look for any signs of compromise and take immediate action, which may include quarantining a device.

Partner with IoT Cyber Security Experts

The security experts at eMazzanti understand the challenges that organizations face when implementing IoT solutions, and we can help. Our network security solutions include automated network mapping and inventory, as well as round-the-clock monitoring. From access management to encryption and more, we provide robust security to counter modern threats.