HITACHI
Inspire the Next

10 QUICK TIPS TO SECURE YOUR IOT ENVIRONMENT

Robust Authentication

Authentication that is robust and effective is Security 101 for the IoT. Make sure that you change default passwords and manage hard-coded passwords appropriately across your IoT network.

Encryption and PKI

Encryption is a fundamental method to protect data at rest and in transit. Any Internet-enabled or other connected device-based system must use Public Key Infrastructure (PKI) and encryption to ensure safe communication, data security and software integrity.

Security Logging

Security logs can give you an early warning about a security issue or they can give you the evidence to determine the cause of a security incident. Make sure that you can collect security logs across your IoT infrastructure.

Mobile Apps (for IoT Devices)

Many IoT devices are associated with mobile apps. Security measures must extend to any connected apps. If at all possible, set in place second-factor authentication to access the mobile app and ensure transport encryption.

Universal Plug and Play (uPNP)

Universal Plug and Play is a discovery protocol to allow devices to automatically find other devices on a network. It is important to either not use uPNP at all or (if you must use it), ensure that device firmware is always fully patched and up to date.

Firmware and Patching

Vulnerability management is essential for all applications, and IoT devices and related services are no exception. You must always keep the firmware patched and up to date.

Physical Security

Device physical security is also important to include in your IoT security strategy. Physical security is not just about the protection of a device. Another aspect of the IoT is the use of sensors that generate data. The integrity of these data depends on the physical protection of the sensors.

Be Cloud-Aware

IoT devices are not islands. They link up across Cloud infrastructure and the data they generate flows across, and in and out, of the connected parts. Cloud security is paramount, and you should consult your Cloud provider to ensure adequate data protection and monitoring processes to secure your IoT environment.

Good Research

Security should be an integral part of the design remit of the manufacturer/ supplier/ deployer. Look at areas such as the use of secure-coding techniques, code analysis, and vulnerability testing.

Device Inventory

Knowing which devices you have in play is essential. An inventory of devices also allows you to map data movement. This then feeds into security policy and strategy – giving you the knowledge to know where to put technological measures in place to prevent data exposure and close off vulnerabilities.

Hitachi Systems Security Inc.

www.hitachi-systems-security.com
+1 866-430-8166
@HitachiSysSec
www.linkedin.com/company/hitachi-systems-security