IoT Security Checklist for Properly Protecting Connected Solutions

Introduction

IoT security continues to be a leading concern among those looking to seek reap the benefits that connected technologies deliver. 32% of IT leaders cite security as the top barrier to IoT success[1], and 82% of IoT adopters say that security is a critical factor in decision making[2]. With these numbers in mind, it is clear that IoT providers must prioritize IoT security to ensure their solutions – and ultimately their customers – are fully protected from potential threats. Even among technology companies, IoT technologies present unforeseen challenges when it comes to security, and many organizations struggle with several key areas critical to IoT security:

- Treating Security As An Afterthought – many device manufacturers today fail to design their products with security in mind, with IoT security prioritized below speed-to-market and revenue. For the best results, developers should be dedicating resources to securing the device from inception to ensure any potential risks are identified and addressed as soon as possible.
- Applying Traditional IT Knowledge to IoT – traditional IT and IoT security vary in many ways – with a major differentiation being that IoT devices are connected to the physical world. Additional differences include device environments, device and network varieties, and deployment volumes. It should also be noted that IoT bridges information systems and operational systems which may have different existing security protocols that must be merged.
- Underestimating Resource Requirements – IoT deployments are typically designed to scale, with many reaching hundreds of thousands connected devices. Ensuring properly managed, end-to-end security for each individual solution requires dedicated resources with deep security expertise. For a larger implementation, an entire IoT security team is optimal for reducing the risk of costly security breaches.

The complexity of these IoT security challenges can be simplified through the creation and execution of a carefully planned, thorough strategy for protecting all components of an IoT implementation. To help get you started, the checklist below can be used as a guideline for ensuring a strong foundational approach to IoT security.

Only 50% of companies considering an IoT implementation say they have the internal skills to manage security[2]

Device Layer – refers to the security of the endpoint device of an IoT solution that collects and transfers data to other devices and systems.

- □ Ensure that physical access does not allow theft or intrusion
- □ When possible, generate unique usernames and passwords and do not use default credentials
- □ Update passwords regularly and do not use devices with hard-coded passwords
- □ Monitor user authentication and authorization to ensure proper access control, and be sure to log both successful and failed attempts to access the device
- □ Shut down unnecessary device capabilities (i.e. camera, microphone, etc) to limit potential areas of exposure
- □ Ensure the device supports encryption of sensitive data at rest and application layer security
- □ Leverage firmware and software that can be updated regularly to reduce vulnerabilities
- □ Implement secure booting to ensure only verified software can be used on the device
- □ Avoid the use of public/static IP addresses

Communications Layer: Network Infrastructure – these activities are typically verified by your network connectivity provider and can be used as a guideline for partner selection.

- □ Implement best-in-class network firewalls and Intrusion Protection System (IPS)
- □ Regularly update infrastructure with the latest security patches, ensuring they are applied in a timely manner
- □ Implement cybersecurity management framework based on ISO27001
- □ Secure and authorize physical access to servers and network components (PIN code, ID badge, biometrics, etc.)
- □ Conduct annual, third-party security and risk assessments
- □ Scan networks for vulnerabilities daily, and ensure scan results are reviewed by qualified security personnel (i.e. Security Director, Security Analyst)
- □ Maintain security event logs for historical reporting
- □ Implement 24x7 security event monitoring by SOC (Security Operations Center)

Communications Layer: Data Transfer – refers to the protection of in-flight data and secure transfer among connected devices and other systems.

- □ Implement a site-to-site VPN solution to allow for encrypted data transmission to limit exposure to the public Internet
- □ Implement a data signing solution to ensure authenticity and integrity of transmitted data
- □ Ensure continuous data traffic monitoring for anomaly/event detection
- □ Implement alerting tools for automatic fraud prevention

Application Layer – refers to securing the application and databases that allow an IoT solution to function as expected.

- □ Implement code analysis tools to automatically inspect application source code and identify vulnerabilities prior to pushing to production
- □ Adopt a mindset of “Security by Design” into the SDLC
- □ Ensure timely, automated application updates to protect against evolving security risks and new virus attacks
- □ Use key exchange tools to enable secure updating of IoT application security keys
- □ Leverage certificate enrollment tools to assign each IoT device with a unique identifier, which must be verified before accessing networks and systems

Conclusion

This checklist covers the most critical elements of IoT security, but it is important for organizations to honestly assess what they are capable of executing internally and where they may need added resources. Because many companies lack internal expertise, may have insufficient resources, or face challenges with unfamiliar IoT security practices, it is often beneficial to engage a trusted IoT partner.

66% of companies include external vendors on their IoT planning teams[3]

There is no one-size-fits-all solution for IoT security, however businesses should seek a partner that can deliver deep IoT experience to guide strategic IoT security planning, best-in-class security management capabilities, as well as the products and professional services needed to safely move your IoT project forward.

Reach out to KORE today to learn how we can help you navigate the complexity of IoT security

Sources

1. Gartner – Leading the IoT
2. Vodafone Barometer
3. http://info.forbes.com/rs/790-SNV-353/images/Hitachi%20IoT%20Report.pdf