PONDURANCE

Understanding the Top Five IoT Security Challenges and How To Reduce Risk

In designing and building new Internet of Things (IoT) technologies, security must be a pivotal part of the product's life cycle. As organizations adopt these new technologies, security implementation must be considered a foundational element in the adoption process. This could be easier said than done for most IoT manufacturers because of the minimal security requirements and the minimalist nature of IoT.

With this much data floating around, sensitive data is at risk, and it is no surprise that IoT devices are prime targets for cybercriminals. IoT is a technology and market with nonexistent security or compliance requirements. As these devices continue to collect massive amounts of data, consumers in California and Virginia have consumer privacy regulations in place to stop the sharing and selling of their personal data associated with these devices. But what about regulations that require manufacturers to enact a minimum set of security requirements during the design, creation, and testing of these products?

IoT devices generated **17.3 ZB of data** in 2019 and expected to increase 20% by 2025.[2]

IoT was designed to simplify our lives from a consumer perspective; however, it introduces many more cybersecurity risks. Therefore, it seems like it would be easy to secure this technology that has impacted our lives in many ways. As a result of a complex and ubiquitous ecosystem, it is not easy to secure this technology. While the majority of the security risks associated with IoT devices are with the manufacturer, users can still broaden the risks by ignoring updates and user guides.

For users to better understand the cyber risks associated with IoT devices, it is important to highlight the top security challenges that organizations should be aware of:

NONEXISTENT SECURITY COMPLIANCE REQUIREMENTS

The IoT industry was valued at $212 billion worldwide in 2019[1] and is expected to reach $1.6 trillion by 2025. For most manufacturers, security is not the top priority when it comes to a first-to-market mentality, and other companies have created businesses leveraging IoT data to improve consumer behavior advertising trends. In fact, IoT devices generated 17.3 zettabytes[2] of data in 2019, and that number will increase by 20% by 2025.

PROBLEMS IN FIRMWARE UPDATE MANAGEMENT

While tried-and-true methods that have been used to detect vulnerabilities in other software infrastructure may reduce cyber risk, IoT systems are more complex due to the diversity and ubiquity of devices and communications. Although vulnerability detection may be necessary, it is not the only firmware-related security requirement needed to stop attacks. Security as a foundation for firmware development needs to start with the designer and continue through the manufacturer.

Basic security vulnerabilities such as stored encryption keys or passwords should be mitigated by initial design and verified by continuous testing. Firmware updates can be complex because IoT devices are not always connected to the internet, resulting in difficulty signing updates. It is important that updates are signed to prevent the devices from being erroneously updated with potentially malicious code.

In addition to firmware challenges, the physical security of devices must be considered since they can be easily accessible. Physical interfaces such as the Joint Test Access Group (JTAG) interface can be used to physically attack IoT devices[3] as a backdoor entry point to gain root access. This attack method can be simplified by using a tool such as a JTAGulator, which can connect to the JTAG interface of a device and send serial commands to take over the device. Exploits like these can impact a human life when it comes to patients relying on IoT devices to power life-saving medical equipment.

HIJACKING IOT DEVICES

IoT manufacturers often leave well-intentioned backdoors open in these devices to provide ease of access for technical support or updates. However, these backdoors are easy for threat actors to exploit, and they can look up publicly available default passwords to gain unauthorized access to the sensitive data stored and gathered from these devices. All default credentials or accounts should be disabled before devices ship.

In the past, threat actors have used IoT devices to deploy IoT botnets[4] for distributed denial of service (DDoS) attacks. In addition to DDoS, attackers often use IoT to gain access to an organization's network or as a form of spyware[4] to deploy spearphishing attacks and listen to private conversations among a company's key stakeholders.

IOT IN THE WORKPLACE

IoT is widely used in the healthcare, manufacturing, and industrial sectors to improve logistics. Organizations rely on IoT data to drive real-world decisions, which can lead to poor business decisions if the data is disrupted or altered by a threat actor. As previously mentioned, IoT can broaden the attack surface within a business and is a soft entryway for cybercriminals to gain access to an organization throughout the supply chain.

As organizations adopt IoT in the workplace, securing the data and the entire IoT ecosystem should be a critical business function. IoT devices can directly access technology on the internal network, such as wireless access points and HVAC systems, and gather IP addresses, which can lead to much larger issues such as putting human lives at risk. At times, instead of working for us, IoT devices can work against us and provide too much information or access to cybercriminals.

KEY STEPS TO REDUCING IOT SECURITY RISKS

Being aware and understanding the risks involved with using IoT devices are steps in the right direction. Some critical steps to protecting your business and consumers from the vulnerabilities found in IoT devices need to start with visibility into all the IoT devices being used within your organization:

- **Inventory management** is critical when using IoT tools to improve business value within your organization. Having an accurate count of how many and which devices are used and isolating your inventory by air-gapping them on your business network is essential to reducing the risks of IoT devices accessing sensitive parts of your network.
- **24/7 monitoring** of your network, logs, cloud infrastructure, and IoT devices is vital to ensure you are effectively monitoring, detecting, and alerting the security team when malicious behavior is detected. If your organization does not have the staffing to monitor around the clock, businesses are turning to Managed Detection and Response (MDR) services to act as a trusted security advisor or as an extension of your security team.
- **Risk assessments** are valuable when you work with outside vendors. There are different types of risk assessments such as vendor risk assessments, pen-testing to check for vulnerabilities within your IoT devices, and privacy risk assessments if you are using IoT devices to gather information for marketing purposes.

IoT use in healthcare, manufacturing, and industrial sectors **improves logistics.**

- **Firmware updates** are always critical to ensure vulnerabilities are updated and patched by the IoT manufacturers. It is important to communicate security updates with supply chain management to ensure transparency in any security updates with other vendors or clients.
- **Multifactor authentication** is an added level of security that should be activated if your IoT manufacturer offers this option. It is important to update the default password to something more secure and have a dedicated account manager to manage the multifactor authentication when accessing or managing IoT devices within your organization.

The IoT is an incredible platform for innovation. However, IoT will continue to open opportunities for new online threats. As with any new technology, strong security is essential. A standardized approach is needed based on established principles to ensure it is as secure as possible.

We recommend establishing tools and programs in alignment with the NIST Cybersecurity Framework. It is also key to have prevention, detection, and response plans in place such as those plans that MDR services provide. Most importantly, having a disaster response plan is key, and not just for cyberattacks but also for business situations where malfunctioning IoT or inaccurate data would cause damage. At Pondurance, we recommend having 24/7 security monitoring in place to detect unwanted behavior and reduce the likelihood of an incident.

ABOUT PONDURANCE

Pondurance delivers world-class Managed Detection and Response services to industries facing today's most pressing and dynamic cyber security challenges including ransomware, complex compliance requirements and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts we continuously hunt, investigate, validate and contain threats so your team can focus on what matters the most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment and more unified risk management for their organizations. Visit Pondurance.com for more information.

Sources:
1. IoT Trends in 2021: Is IoT worth the buzz?, Intelisa, Jan. 2021.
2. Re-Hashed: 27 Surprising IoT Statistics You Don't Already Know, Hashed Out by the SSL Store, Feb. 2021.
3. Exploiting JTAG and Its Mitigation in IOT: A Survey, MDPI, Oct. 2018.
4. Mirai botnet adds three new attacks to target IoT devices, ZDNet, May 2018.