WHITEPAPER

Mitigate IoT risk with proactive security monitoring

Five core IoT security challenges and how to address them

KORE

Published by

MOBILE WORLD LIVE

Introduction

The Internet of Things (IoT) creates fresh opportunities to launch innovative products and services as well as to tap into new income streams and business models.

IoT technology is already transforming industries such as insurance, manufacturing, healthcare, logistics, fleet management, construction, automotive and others but it's early days, and the majority of the potential value remains untapped.

The IoT market is set to be worth $1.6 trillion worldwide by 2025 – up from $164 billion in 2018 – representing an increase of almost ten-fold. During the same period, the total installed base of IoT-connected devices is projected to reach 75.44 billion globally.

These devices, underpinned by ubiquitous connectivity, create new ways to save money, do things more efficiently, and better meet customer demands and expectations.

Balancing opportunity and risk

In short, IoT represents a huge opportunity to expand or even reinvent your business and those of your customers. This is particularly important in many traditional industries facing pressures to reduce costs, up productivity and stay relevant in a fast-changing world.

However, this opportunity also brings new risks and liabilities related to privacy and security.

We are seeing a seemingly never-ending stream of headlines about data leaks and hacks, with companies as diverse as retailers, hotel companies and even banks affected. Although they're not all IoT-related, these cases show the reputational and financial damage that can ensue from cybersecurity breaches. Earlier this year, for example, Equifax estimated it had spent $1.4 billion recovering from its 2017 data breach, which exposed the personally identifiable information (PII) of 148 million customers.

When an IoT device is connected to a cellular network, there are additional cost implications associated with unexpected data usage that occur when a device is compromised.

However, with IoT products and services, the stakes are higher still and go beyond financial aspects. Because IoT solutions interact with the physical world, an IoT network security breach could result in injury or damage to property. These risks are particularly high when an IoT application is used to monitor critical infrastructure, such as in industrial or utilities settings and smart cities.

Other IoT solutions, such as those integrated into ATMs, security systems and Personal Emergency Response Systems (PERS) devices, transmit confidential information over the network. Unprotected segments of the network could be open to attackers, leaving sensitive data vulnerable. Research suggests, for example, that personal healthcare data is three times more valuable to hackers than credit card information.

Security by design

The challenges to securing IoT solutions are significant but by no means insurmountable.

Organizations are often under pressure to get their IoT solution to market quickly, meaning security is sometimes an after-thought. While comprehensive security measures may delay release schedules and increase costs, failing to do so is a false economy. It is much more expensive to try to secure the solution at a later stage – or to deal with the fallout of a breach.

A holistic approach is key. This isn't easy given the variety of technology components involved in deploying IoT solutions, as well as lack of standardization. As different sensors, SIM types, software and networks are introduced, the effort required to maintain security through monitoring and patching increases.

Leading companies manage security as a strategic issue. By establishing the right policies and processes, deploying automation tools and working with expert partners, companies can ensure IoT security by design.

SECURITY IS TOP OF MIND

42%

of enterprise executives say security is their top IoT concern

55%

of consumers across the US, Canada, Japan, Australia, France and the UK do not trust their connected devices to protect their security

79%

of manufacturers globally say they have suffered some form of IoT cyberattack in the past year – operational downtime (47%), compromised customer data (35%) and compromised end-user safety (33%) were the most common impacts

Mitigating the top five IoT security risks

Security threats can never be removed altogether – successful security strategies are about risk management, which includes the ongoing process of identifying risks and taking steps to mitigate them.

Threat modeling can help you evaluate the individual risks associated with a particular solution and implement measures to protect against them. Once solutions are deployed, holistic oversight alongside policy-driven automated alerts and responses are key to keeping services running seamlessly and securely.

While each IoT solution and system has its own security requirements, there are some common fundamentals to be aware of.

Risk 1: Device or SIM theft

Non-embedded or hardwired SIMs and devices are vulnerable to theft, particularly when they are deployed remotely in the field and physically unmonitored, as many IoT solutions are.

In 2018, a Polish charity received an unexpected phone bill for $2,700 after a GPS tracker being used to track a stork's migration patterns was stolen by someone who used it to make hours' worth of phone calls.

In an earlier case, thieves in South Africa ripped SIM cards out of traffic lights, leading to not only a high bill and replacement costs of around $1.26 million but also traffic jams and accidents.

Experts suggest there could be a burgeoning black market for SIM cards and IoT devices would be an easy target.

SIM-jacking is also on the rise. SIM-jacker attacks involve an SMS containing a specific type of spyware-like code being sent to a mobile phone, which then instructs the UICC (SIM Card) within the phone to 'take over' the mobile phone or IoT device in order to retrieve and perform sensitive commands.

eSIMs are on the rise to boost security as well as flexibility but they are not risk-free. The number of embedded SIMs (eSIMs) in use is expected to grow from 108 million in 2016 to nearly 1 billion by 2021. SIM cloning is an ongoing threat with eSIMs, as is eSIMS on discarded or unguarded devices being recalibrated and used for nefarious purposes.

Remedy: In the case of device or SIM theft, you need to act fast – before the bill shock hits. Crucial to this is establishing and managing authorized access to certain devices, firmware and geographic or regional areas. Real-time alerts and remote provisioning can quickly shut down stolen property when one of these violations occur. IMEI change detection can automatically trigger rules and security measures.

Risk 2: Excessive data use

Anomalies or spikes in data usage can indicate a security breach – or unauthorized use, including mobile streaming.

When an IoT device is connected to a cellular network, an organization may be financially viable for all the costs associated with unexpected data usage that occurs when a device is compromised. If an IoT device that infrequently transmits data is hacked and begins transmitting a high quantity of data, any overage is billed by the mobile network operator.

This can happen when an IoT device becomes part of a botnet and is used in a distributed denial of service (DDoS) attack. Research suggests that a DDoS cyberattack could cost companies between $50,000 per attack and up to $2 million for large enterprises.

A DDoS attack can be initiated by crawlers that identify IoT endpoints that are not secured properly or contain exploitable vulnerabilities. For example, an attacker could develop an application that scans for devices where the default administrator password has not been changed. The application can then install malware on the devices and the malware could transmit a large amount of data. When this happens, an otherwise inexpensive-to-operate device incurs a large number of cellular network usage charges. The financial impact of this attack can be substantial, incurring hundreds of thousands of dollars in overages in some cases.

DDoS attacks most often occur because basic security hygiene is

neglected. Organizations can help prevent such attacks by diligently managing usernames and passwords. It is important to mandate that strong passwords are used and that they are changed frequently.

Another preventative measure, wherever possible, is to deploy IoT devices behind a firewall, not on the Internet with a public/static IP address.

Still, even with the best intentions, hackers are always looking for new ways in. If your organization is infected with a DDoS attack, it is important to know immediately.

Remedy: Network anomaly detection tools, programmed with burst detection rules, can alert you to changes in your usage before data is stolen or your costs dramatically increase.

For example, if a device commonly sends five megabytes of data per month, monitor to ensure that it stays within that baseline. If the device transmits data in excess of the chosen range, it can be programmed to be deactivated or suspended immediately.

Risk 3: Network or device failure

In the rare instances that the network fails, data and IoT services are at risk.

In December 2018, 02's network went down for a day in the UK due to a software glitch. The outage meant 32 million users of O2, GiffGaff, Lyca Mobile, Sky Mobile and Tesco Mobile in the UK had little or no data and SMS services for an entire day. It also affected card payment terminals and public transport systems – Transport for London's (TfL) real-time bus updates were unavailable, for instance. Journey-planning apps such as Google Maps or CityMapper could not receive data from buses via 02 networks. Elsewhere, mobile payment apps for services such as parking, public transport and bike hire were also impacted.

In most cases such as this, network outages are inconvenient.

However, in some applications, device or network outages could potentially mean loss of revenue, damage to equipment or even risk to life. Consider critical IoT-connected infrastructure in smart cities, such as traffic control, or connected healthcare devices used by individuals.

Remedy: IoT systems must have redundancy built-in and be resilient against single points of failure.

You can only take action when you are quickly made aware of network or device failures. Outage detection rules plugged into automated tools can trigger failover systems and data suspension instantly.

Risk 4: Anomalous communication patterns

If devices suddenly start transmitting to a new or unauthorized destination, data is at risk.

A recent report from Zscaler analyzed millions of connections from IoT devices on enterprise networks, including IP cameras, smartwatches, smart printers, smart TVs, set-top boxes, digital home assistants, IP phones, medical devices, digital video recorders, media players, data collection terminals, digital signage media players, smart glasses, industry control devices, networking devices, 3D printers and even smart cars and found that in over 40 percent of cases, traffic was not encrypted.

The research also revealed that 91.5 percent of data transactions performed by IoT devices in corporate networks were unencrypted.

This could leave systems vulnerable to 'man-in-the-middle' (MitM) attacks where hackers intercept traffic to steal or manipulate data.

Remedy: IoT encryption is essential. If your IoT solution collects and processes sensitive information such as PII, the data should be encrypted both at rest and in transit.

A common reason for the lack of encryption is the limited memory and processing power of many IoT devices. One way to overcome this is to offload encryption functions to a network or cloud provider which uses a virtual private network (VPN) to encrypt data and transmit it securely, regardless of device limitations.

In addition, as well as implementing rules to restrict data from being sent to unauthorized locations, you should also create alerts to bring this to your attention quickly should it happen.

Risk 5: Lack of visibility as a whole

Successful IoT deployments require a mixture of the right devices, networks and encryption, and security must be maintained throughout the IoT solution lifecycle and at all touchpoints. This intricacy can make it challenging to isolate the cause and location of security issues quickly as well as to retain holistic oversight.

Complexity is set to increase further too – according to Gartner, by 2023, the average CIO will be responsible for more than three times the number of endpoints they managed in 2018, with much of this growth coming from IoT devices.

Recent research by Forescout found that 49 percent of UK businesses – up to 2.8 million companies – believe there are unknown, third-party IoT devices on their network, a two percent increase since 2018. This is despite the fact that 85 percent of the CIOs and IT decision-makers questioned by Forescout said this poses a security risk to the organisation.

A worrying 15 percent they were unaware that a lack of visibility and control of these devices leaves network security infrastructure weakened. While 58 percent of respondents thought a centralized approach to security would protect against vulnerabilities in the security infrastructure, only 49 percent had implemented any such strategy in their organizations.

Remedy: Achieving the required cybersecurity oversight requires a mix of skills, technology and processes.

A 2018 Vanson Bourne survey found that 60 percent of enterprises said they have an IoT skills deficit in cybersecurity and 46 percent reported a deficit in data analytics talent – these were among the reasons that 74 percent said they planned to work with external partners to facilitate IoT deployment and growth.

With their deep expertise and market experience, an experienced IoT partner will able to identify the proper IoT wireless network infrastructure technologies to support effective, scalable IoT solutions. Importantly, they will also be up-to-date with the latest best-in-class security measures and will constantly scan the horizon to deliver cutting-edge security technologies.

For example, some of the latest solutions include purpose-built cloud IoT networks and VPN services which enable end-to-end encryption of all in-flight data traffic as well as tools for proactive security monitoring, alerting and reporting, and mitigation in real-time.

TOOLS FOR THE TASK: KORE SECURITYPRO

Problem to be Solved	SecurityPro Solution
Firmware/Application Misconfiguration	Destination IP, Protocol and Port Change Rules
Stolen SIM	IMEI Change Detection
Network or Device Failure	Outage Detection Rule
Lack of Visibility for Device Communications	TrafficStreamer and Traffic Reports
Excessive Data Use Due to Security Breach	Burst Detection Rule

Conclusion

Security risks won't go away – hackers will only become more inventive and sophisticated alongside IoT developers. 'Micro-breaches' are predicted to be a growing trend, whereby instead of launching large-scale dramatic attacks, hackers will more subtly leak data to avoid detection.

This reinforces the importance of a holistic security approach, encompassing people, processes, partners and technology.

Leading IoT providers will be those that balance security alongside innovation and that take a strategic approach to effectively managing ever-changing threats. Some fundamental principles apply:

- Reduce the risks associated with introducing new technologies by having a standard vetting process in place for vendors and products at each level of the technology stack.
- Diligently manage usernames and passwords. It is important to mandate that strong passwords are used and that they are changed frequently.
- Whenever possible, deploy IoT devices behind a firewall, not on the Internet with a public/static IP address.
- The best way to ensure robust security measures in an IoT solution is to perform threat modeling during design. Threat modeling begins with an architecture diagram of the solution that depicts how data flows throughout the application's different elements. This allows you to identify, document and score the most likely attack vectors, then determine the mitigation steps accordingly.
- In the event of a cybersecurity incident, it's essential to know immediately. Deploy network anomaly detection tools to monitor for any changes in behavior and activity, such as data spikes or unauthorized access or communication patterns. Automated actions can be deployed instantly to limit the attack and potential damage.
- Consider working with an experienced IoT partner with in-depth expertise to help you curate the optimal mix of SIMs, network connectivity options and other technology components to achieve business goals while ensuring that security is engineered into any IoT solution by design. The right partner will also work with you to map out appropriate policies, procedures and tools so that security can be managed effectively once the solution is live.

About KORE

KORE is a pioneer, leader, and trusted advisor delivering transformative business performance. We empower organizations of all sizes to improve operational and business results by simplifying the complexity of IoT. Our deep IoT knowledge and experience, global reach, purpose-built solutions, and deployment agility accelerate and materially impact our customers' business outcome.

About KORE SecurityPro

KORE SecurityPro is a network diagnostic and troubleshooting tool that enables organizations to monitor and secure the traffic of their IoT connections on a device level, with the ability to easily set rule-based alerts and notifications. An adapative network-based security solution, KORE SecurityPro provides the network visibility and actionable intelligence that connected organizations need to protect their IoT devices and the data they transmit from potential anomalies, reducing costs and mitigating security risks.

Find out more www.korewireless.com

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What's more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this whitepaper are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries.