Unsplash © JJ Ying

IoT: An Internet of Threats?

The Internet of Things promises an advanced environment where every object is intelligent and connected. However, are these devices secure? What security risks do they pose, and how can businesses and individuals alike take advantage of IoT safely and securely?

IoT promises a new age of connected objects. The ecosystem IoT creates is far-reaching from manufacturing as Industry 4.0 continues to evolve to smart homes and cities that rely upon an integrated system of digital devices that create an immersive ecosystem. However, is IoT secure? What are the potential risks businesses and individuals should be aware of?

According to research from *ABI,* there will be an estimated 8.6B connected devices by 2026. With this level of expansion, ensuring security is at the foundation of IoT is critical, but is the industry paying enough attention to this as they create new devices?

The annual 2021 SonicWall *Cyber Threat Report* has a wide-reaching overview of cybersecurity. This year's report factors in the security issues that the pandemic has exposed and exacerbated.

"In March 2020, masses of employees packed their personal office belongings and equipment to work from home for months on end, simultaneously creating an explosion of new attack vectors," the report states.

> *“In 2020, SonicWall Capture Labs threat researchers recorded 56.9M IoT malware attempts, a 66% increase that showed shifting tactics for lurking cybercriminals.”*

Also, the UK was the fourth worst-affected country for ransomware with 8.5M attacks, making up 4.2% of all global attacks. And as workforces moved to their homes as the pandemic took hold, IoT devices became the backdoor for hackers, with attacks jumping 48% across Europe.

Palo Alto Networks’ *study,* which polled businesses across 14 countries, concluded that 57% of IoT devices are vulnerable to attack. The report goes further, revealing that many companies are struggling as they try to apply robust IoT security practices. Only one in five (21%) of the IT decision-makers surveyed reported having implemented the best procedures of using micro-segmentation to contain IoT devices in their own tightly controlled security zones.

The range of IoT devices being deployed is massive and spans every industry and sector from healthcare to agriculture. With such a broad deployment landscape, securing these devices can be a challenge.

Unsplash © NASA

Speaking to *Maddyness*, Candid Wüest, VP cyber protection research at Acronis, explains the dilemma that often influences how security IoT is approached: “Security and privacy are unfortunately still not a high priority for most IoT devices. This holds true for both the vendor side and the consumer, which is not asking for security or is rarely willing to pay more for additional security features.

“For most end users it is impossible to judge the security level of a product from the packaging. This is one of the reasons why various user associations are asking for certifications and simple to understand explanations on IoT products. The wide integration of 5G into IoT might increase the number of devices that are reachable directly from the Internet, which could lead to more compromised IoT devices being used as part of a botnet, for example to conduct DDoS attacks.”

Digital ecosystems

The rollout of 5G has accelerated the development and deployment of IoT devices. Whether to support the transformation of manufacturing or ushering in the age of the smart city and intelligent home, the digital environments being created are often not paying close attention to the security that these networks and devices must contain.

Few consumers understand the attack vectors that are being developed as the IoT ecosystem expands. An IoT equipped toaster should just work and include integrated security protocols, but this is often not the case.

Not all IoT devices are made the same. This can be a significant contributing factor to the level of security some IoT devices have built into them. The *GSMA* made this clear in their report stating: “Many IoT devices are designed to have low power consumption, to be low complexity and low cost, to have a long life duration and to operate outdoors. Low-cost IoT devices may have limited cryptographic capability, small memory and constrained operating systems.

“The result is that the device may be unable to perform ‘internet-grade’ cryptography or contain ‘secure hardware’ and they could be subject to physical or localised attack that could compromise the security and privacy of data stored in them.”

Keeping each device’s security protocols up to date isn’t something consumers have an appetite for. More worrying is that a vast number of IoT devices will be autonomous.

M2M (Machine-to-Machine) communications are essential to creating service networks that everyone can use.

However, without comprehensive and robust security updates, these human-free networks can be vulnerable to attack. The need to seamlessly connect to the available network offers great convenience yet can also open the door to malicious attacks.

Reza Moqadasi, global head of IT at ITRS Group, told *Maddyness* better security is coming: “Most efforts are organised at a national level. For instance, in the

past two years as part of the UK Government's *National Cyber Security Strategy,* a review was conducted into how to improve the cyber security of consumer IoT products and associated services.

"The initiative, which was dubbed 'Secure by Design', led to the formation of a *Code of Practice* for IoT manufacturers and developers. By ensuring that global trading partners adhere to the same best practices, it may be possible to get a head start in mitigating the privacy and security risk to IoT consumers."

Unsplash © Joshua Rodriguez

New security

Steps are being taken to make IoT security an integrated and standard component of these devices. The FIDO (Fast IDentity Online) Alliance recently announced their *FIDO Device Onboard* protocol that aims to solve IoT security issues in onboarding – just as it has done with its FIDO authentication standards to help address the global data breach problem.

The FDO specification has reached Proposed Standard status and is open and free to implement. Initially, the specification is targeted at industrial and commercial applications.

"The FIDO Device Onboard standard builds on the Alliance's ongoing efforts to help close the security gaps that currently exist on the web, by expanding this work into IoT applications," said Andrew Shikiar, executive director and CMO of the FIDO Alliance.

"Businesses recognise the huge potential of the IoT and the enormous benefits it can bring to manufacturing, retail, healthcare, transportation, logistics and more. The paradigm needs to shift immediately so we can move IoT technologies ahead with safer, stronger and more secure means of authentication for these important uses in industrial and commercial environments."

With Dave Kleidermacher, VP, Android security and privacy at Google also commenting: "The work the FIDO Alliance is doing to address phishing by closing security gaps on the web would not be possible without industry collaboration and standardisation. It's a natural fit for the FIDO Alliance to use these same tools to address the threats against IoT infrastructure. As a board member of the FIDO Alliance since its earliest days, Google is proud to have contributed to this new standardisation effort to better secure IoT."

This initiative is also joined by the UK government's recent announcement that

new cybersecurity legislation aimed primarily at protecting intelligent devices is a priority.

Commenting on this development, Joseph Carson, chief security scientist at Thycotic, says: “The new UK law to improve security on smart devices is a welcome step in the right direction, however, it must go further to ensure that it includes security best practices that are part of the solution.

“Transparency is critical, so when purchasing a new smart device, it must be clear on how long the vendor continues to provide security updates, just like a manufacturer warranty period or an expiration date. This type of approach will provide consumers with a clear choice when choosing smart devices comparing one vendor that only provides two- years of security updates versus another that will provide five years.”

The ongoing approach is also supported by the ITRS Group’s Reza Moqadasi, who stated: “The security and privacy challenges around evolution and adoption of new technologies such as 5G or systems such as IoT, underline that the approaches for addressing such challenges need to be focused on the socio-technical domains.

“Cyber security and privacy problems require an interdisciplinary cooperation, where among others, innovators, technologists, social scientists and policy makers can combine their forces for charting a safe way ahead for the adoption of new concepts, technologies and systems.”

Alan Grau, VP, IoT and embedded solutions at Sectigo, concludes that as the IoT space rapidly expands, so should security: “As attack vectors continue to evolve, it is increasingly critical that organisations embrace security solutions that ensure the integrity and security of their IoT systems.

Best-practices for IoT device security include strong authentication and secure software updates – ensuring only authentic code can be installed on the device.

“For a complex system such as Alexa’s Skills that involve the Alexa platform, third-party apps and third-party cloud services – a comprehensive approach to ensuring the security of the ecosystem is essential.”

A balance must be struck to ensure IoT devices continue to deliver the advantages they offer to businesses and consumers alike within a robust security environment. As IoT can damage susceptible networks, a zero-trust approach is needed that forces minimum levels of security across all IoT manufacturers. Here, standards are critical to ensure clear guidance when security is being considered for each new IoT device.

Article by DAVID HOWELL