

TELECOM26 WHITE PAPER

Security for critical infrastructure

The role of IoT and Non-Public Networks

The rapid growth of IoT offers significant business opportunity, but if not secured appropriately, it can also represent a significant security threat and, ultimately, can be used to hijack the corporate intranet.

The Telecom26 solution helps to negate this threat and ensure that your corporate data is isolated from your IoT network to provide an comprehensive end-to-end IoT security solution.

Introduction

Ransomware and Malware attacks are growing - IoT assets are a target

The growing number of Ransomware and Malware attacks is a serious emerging threat for every organisation's security. Unfortunately, the incidences of such malicious attacks are growing and here to stay, so it's vital that all businesses act to protect their networks, data and IoT assets as a matter of priority.



**THE NUMBER OF RANSOMWARE ATTACKS
IN THE SECOND QUARTER OF 2021
WAS NEARLY TRIPLE
THE SAME PERIOD OF 2020**

SOURCE: IT GOVERNANCE

Ransomware attacks are on the rise

According to IT Governance, for example, the number of Ransomware attacks reported in the second quarter of 2021 (to June 30) was 141. To put that in context, that's nearly triple the number reported in the year-ago quarter (55 attacks), and a rise of 42% on the previous quarter (2Q21), during which 107 Ransomware attacks were recorded¹.

No sector is immune, with the Public Sector most affected in 2Q21 (accounting for 24% of all security incidents during that period), followed by Healthcare (23%), Education (13%), Technology (12%), Retail (12%), and Manufacturing (7%)... the list goes on.

IT Governance's quarterly report cites a number of examples of Ransomware attacks during the quarter, including Scripps Health (San Diego's second-largest medical provider), which was subject to a ransomware attack in May whereby hackers stole the personal data of 150,000 individuals and demanded a ransom to remove the malicious code, and the UF Health Central Florida, which suffered a reported ransomware attack that forced two hospitals to shut down portions of their IT network.

IoT devices and sensors are inherently insecure – they are often remote and unmanned, and the outcome of an IoT attack (leading to loss of service) can have catastrophic consequences for both businesses and individuals alike.



THERE COULD BE 35 BILLION IoT CONNECTED DEVICES BY THE END OF 2021

SOURCE: STATISTA

Attacks are growing more frequent and more severe

Meanwhile, computer giant Acer, had the dubious honour of becoming the target of the largest ransom demand to date at \$50 million. Other ransomware attacks halted production at IoT manufacturer Sierra Wireless and beer maker Molson Coors, to name a few.

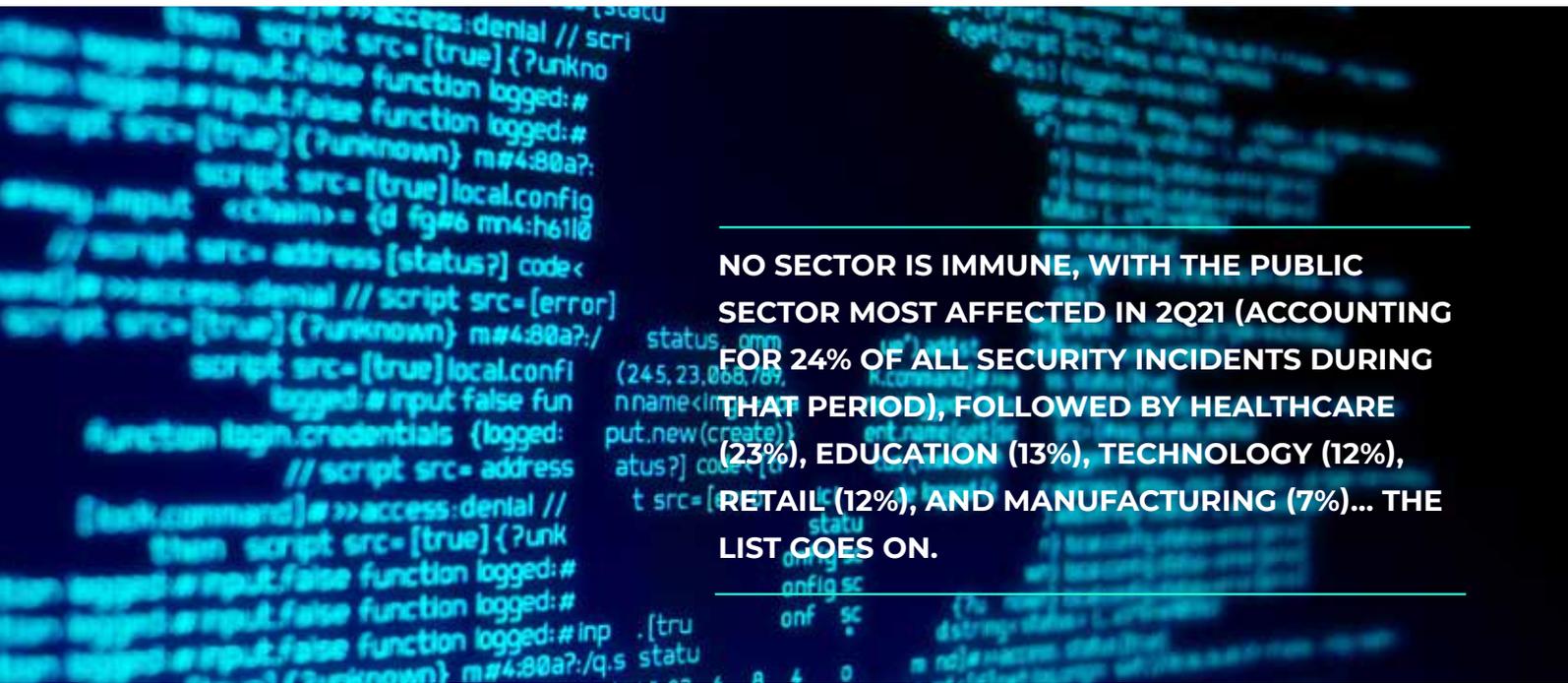
Other reports during the period, include an attack on photographic supplier Fujifilm that resulted in the Japanese multinational shutting down “all networks and server systems” in Japan. It’s reported that Fujifilm refused to pay a significant ransom demand, instead using system backups to restore operations.

Conversely, computer storage supplier ExaGrid has played down reports that it paid a known Ransomware gang, called ‘Conti’, a \$3m ransom. Ironically, ExaGrid supplies backup disk storage equipment that features technology that’s supposed to thwart ransomware attacks.

The growing frequency and severity of Ransomware attacks means that it’s just a matter of time before any company or facility is targeted.

The rapid growth of IoT is part of the problem. It offers significant opportunity for businesses and operators alike – according to Statista, there could be 35 billion IoT-connected devices around the world by the end of 2021². But IoT devices and sensors are also an easy target for hackers.

...computer giant Acer, had the dubious honour of becoming the target of the largest ransom demand to date at \$50 million. Other ransomware attacks halted production at IoT manufacturer Sierra Wireless and beer maker Molson Coors...



NO SECTOR IS IMMUNE, WITH THE PUBLIC SECTOR MOST AFFECTED IN 2Q21 (ACCOUNTING FOR 24% OF ALL SECURITY INCIDENTS DURING THAT PERIOD), FOLLOWED BY HEALTHCARE (23%), EDUCATION (13%), TECHNOLOGY (12%), RETAIL (12%), AND MANUFACTURING (7%)... THE LIST GOES ON.

In the rush to meet the growing demand for, and potential of, IoT services, security has not been applied as a matter of urgency and without appropriate security measures in place.

IoT devices and sensors are inherently insecure – they are often remote and unmanned, and the outcome of an IoT attack (leading to loss of service) can have catastrophic consequences for both businesses and individuals alike.

IoT devices are often connected to the intranet, either directly or via the internet (read on for further explanation), but lack the processing power to apply even basic encryption and other security protection, they are often deployed in their millions, and some devices may even not be registered to, or known by, the IT department due to such large numbers and rapid proliferation. There are also often vulnerabilities in terms of the broader security of new IoT infrastructure, resulting in gaps for protecting legacy systems that may connect to more open environments. In this scenario, a breach of an IoT device can result in unauthorised access to legacy systems.

It means that IoT could become the easiest, and preferred, target for malware and ransomware attacks, which can result in personal and corporate data vulnerabilities. The security of IoT devices is becoming one of the most pressing challenges for organisations and represents a serious vulnerability.

This white paper sets out the security vulnerabilities of IoT ecosystems, and how Telecom26 has the solution to solving this significant emerging security issue.

IoT could become the easiest, and preferred, target for malware and ransomware attacks, which can result in personal and corporate data vulnerabilities. The security of IoT devices is becoming one of the most pressing challenges for organisations



The IoT security threat

Managing the vulnerabilities of IoT assets

As we have seen, IoT sensors and devices often lack the processing power to enable even the most basic security protection. More importantly, they are connected to your intranet, and in some cases – where appropriate IoT security measures have not been put in place – can access internal networks via the internet.

It's essential that organisations understand the threat and respond accordingly – proactively, rather than reactively, by which time it may be too late to repair the compliance and reputational damage caused.

As we will see in later sections, there are technological solutions, such as the one provided by Telecom26, to this threat, however, there are also some basic rules that any organisation can apply to their IoT ecosystem.

What are the IoT security challenges?

A report³ by French technology services company, Thales, lists the six most significant IoT security challenges:

1. Weak password protection
2. Lack of regular patches and updates and weak update mechanism
3. Insecure interfaces
4. Insufficient data protection
5. Poor IoT device management
6. The IoT skills gap

Many organisations operating networks with thousands ... of IoT sensors or devices – may inadvertently be making it easy for hackers to use IoT sensors and devices to breach internal networks as they are often connected to the internet via the main domain, which then enables easy access to the intranet.

On a more granular level, one of the main vulnerabilities is, in fact, an old (but very valid) security issue – the relationship between the internet and the intranet. Modern web browsers provide poor protection against attacks originating from the internet, with hackers easily able to use a web browser as a proxy for the accessing the intranet, or internal network.

Importantly, by using a browser as a proxy, a hacker can not only bypass the perimeter firewall, but also any host-based firewall. Once breached, the perimeter firewall may log malicious code from an external site, but is useless against subsequent attacks on the internal network as these attacks will not go through the perimeter firewall.

Many organisations operating networks with thousands – and even tens of thousands – of IoT sensors or devices – may inadvertently be making it easy for hackers to use IoT sensors and devices to breach internal networks as they are often connected to the internet via the main domain, which then enables easy access to the intranet.

NB – If this is the case in your organisation, it should be changed immediately!

Many IoT sensors use Supervisory Control and Data Acquisition (SCADA) for communications. Typically, SCADA is used for applications and devices that require very low levels of data transmission, at low speeds. It offers a large coverage area. But, conversely, that means that with hundreds – and perhaps thousands – of devices supported in a given location, any attack can have a significant impact.

SCADA does not have strong authentication schemes, particularly when compared to GSM networks, which also offer a smaller footprint (smaller cells) and so any security breach affects fewer devices and sensors.

If data requirements are more significant, then some form of broadband is required, whether fibre, satellite, Wi-Fi, cellular, and so on. Of course, this requires the same strong level of security for vulnerable IoT estates.

So, how can an organisation proactively nullify the security threat that IoT ecosystems represent to your internal networks?

The Telecom26 SIM provides optimum corporate data security whether for greenfield or existing PN deployments. Our unique Telecom26 SIM offers security, reliability, performance, controlled access, roaming and scalability far beyond that offered by any public network, or via network slicing.

A solution to the IoT security threat

Intra-networking to manage your exposure

The ideal solution should provide intra-networking enabled by device SIM access. In this scenario, it's possible to authenticate every device and user, while limiting (or managing) all access to any device or sensor. Because users and devices need to be registered in the HLR / HSS (the databases used in mobile networks to maintain a record of all connected devices and also of those that can be admitted to the network), it means that the network will only handle known (authenticated) devices, while blocking unknown devices and users.

Essentially, SIM-enabled access to the intranet (or private network) – which also blocks the use of internet browser proxies – access points are being limited to the outside world. At the same time, access to individual elements of the network or ecosystem can be disabled in the event of an attack. SIM-enabled sensors and devices can continue to collect data, buffer it, then resume transmission once the security threat has been identified and eliminated.

access to individual elements of the network or ecosystem can be disabled in the event of an attack. SIM-enabled sensors and devices can continue to collect data, buffer it, then resume transmission once the security threat has been identified and eliminated

It's also important to have an isolated backup network – with infrastructure that is completely separate from the primary network. In the event of an attack – as occurred in the Fujifilm incident outlined earlier – it means that everything can be backed up from the isolated network, which should be unscathed following a security event. For example, organisations could use fibre as the primary network, with cellular as a backup, or cellular as primary and satellite for backup.

It's essential, of course, that the secondary isolated backup is a trusted network, by which people, infrastructure, devices, architecture, processes and so on need to be 100% trusted.

If an enterprise owns and manages its own infrastructure, it needs to be trusted, as outlined in the organisation's operations and security policies – the same as a PBX or WAN.

The Telecom26 intra-network solution to IoT security

Manage your devices securely and simply

IoT security, and the intranet / private network (PN) should not be confused with the term 'secure communications' – such as encrypted data that is secure end-to-end. While Telecom26 can offer this, our solution focuses on device management.

WHAT ARE THE IOT SECURITY CHALLENGES?

THALES LISTS THE SIX MOST SIGNIFICANT IOT SECURITY CHALLENGES:



WEAK PASSWORD PROTECTION



LACK OF REGULAR PATCHES AND UPDATES



INSECURE INTERFACES



INSUFFICIENT DATA PROTECTION



POOR IOT DEVICE MANAGEMENT



THE IOT SKILLS GAP

Our SIM-enabled security / device management can be applied to an estate of IoT sensors as easily it can to a mobile workforce and their connected devices and phones. For IoT ecosystems our unique SIM provide a dedicated, secure network for connected sensors and devices, while providing a semi-private network for communications (with fully enabled, secure private / public network roaming).

It means that the communications network is shielded from the sensor network, although with such comprehensive device management and authorisation we can 'force' sensors to connect to the semi-private network when and if necessary. There is no roaming onto private networks, ensuring that your IoT sensor estate is separate and distinct from the private network / intranet, thus reducing the potential for threats from the IoT network.

Telecom26 can also offer similar for organisations using existing public networks for IoT management. For example, a small oil or gas company may not have the resources to deploy and manage an separate PN, but by deploying secure routers and ensuring that data flows through the Telecom26 network, it means that your organisation retains complete visibility and control over each and every sensor and device.

Working with our affiliates and partners, Telecom26 can provide an end-to-end solution for greenfield deployments – from network infrastructure deployment to managed security.

Where the system detects an attempted unauthorised breach to the intranet, the Telecom26 dashboard will sound an alert, allowing administrators to disable and/or block the unwanted security threat – in conjunction with your business and security policies.

The Telecom26 SIM provides optimum corporate data security whether for greenfield or existing PN deployments. Our unique Telecom26 SIM offers security, reliability, performance, controlled access, roaming and scalability far beyond that offered by any public network, or via network slicing. Our solution essentially 'locks down' the IoT estate.

Telecom26 has significant experience in providing optimally secure, high-performance connectivity for both mobile device and IoT estates. We can provide an end-to-end deployment, or we can help manage specific networks, as well as provide advisory services to ensure the best data security possible.

AT A GLANCE

1100+

Network
agreements

200+

Countries &
territories

650+

Unique mobile
operators

1

SKU

Conclusion

An IoT network that's secure by design

Telecom26 has exceptional pedigree in helping organisations to build, deploy and securely manage their private and semi-private networks that help to connect the entire infrastructure. We can help you to build independent, private networks for your IoT estate and/or mobile workforce.

Our unique SIM-enabled solution means that your internal network is isolated from attacks via IoT sensors and devices. Where sensors are connected via the public internet, we ensure that the connection is via a secure VPN.

Telecom26 works with a network of partners and affiliates that can provide an end-to-end, comprehensive private network or, at the other end of the scale, we offer a SIM-enabled solution (which can be a single SIM or dual SIM – for example, for devices that need to roam between the public network and a private network) – that can ensure that your IoT infrastructure is no vulnerable to attacks that attempt to access your corporate intranet.

With hackers targeting the often weak security of IoT sensors and devices, it's essential that all organisations ensure that their IoT networks are not only secure, but isolated from the corporate network, and are backed up on a trusted isolated network for backup should the need arise.

Get in touch with us today, to find out how we can help to secure all your networks, whether for communications or for IoT data streaming.

We are the only provider that can offer secure roaming between public and private networks (with managed corporate security) through our dual Telecom26 SIM... all on a single bill.

References

Footnotes and attributions

1. <https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q2-2021>
2. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
3. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats>



Telecom26 AG.

Bahnhofstrasse 10, 6300-CH Zug,
Switzerland

+41 43 500 42 44

www.telecom26.ch