We need to talk about this IoT thing...

Gemserv

INTRODUCTION

In this paper we examine changes that may need to be made to the way we manage our security processes, to prepare the groundwork for the Internet of Things (IoT) and the security challenges it brings. We look at some of the market drivers of the IoT, regulations and initiatives, organisational and technical changes ahead; and finally, why we should stop calling it the IoT.

In fact, let's do the last bit first. Why should we stop calling it the IoT? The term IoT has simply become too vast, there are too many architectures, too many technologies, too many use cases fall under its umbrella. Trying to define "IoT" security is simply too vast a subject to contemplate. We prefer the term Connected Device (the acronym 'CD' is up for re-use). Its not really any better than the term IoT, and likely even more vague, but it's easier to think about the security of a CD; and if that device connects to other devices, we need to think about the next link in the chain, a ground up approach.

Of course, the added complication is that CDs can range in functional capability from an internet connected gateway device (running a standard operating system and closely resembling the traditional IT devices such as desktops and laptops); to single function devices, running bare metal (no operating system). The location and function of a CD must also be considered when defining an appropriate security characteristic. For example, a simple connected temperature sensor used to monitor a domestic property will have one risk profile, however take that same device and use it to monitor the temperature in an industrial greenhouse the risk profile will change. It is these characteristics of CDs that, in our experience, separate them from IT and why we may need to make a few changes to our business and technical processes to efficiently administrate CDs as they continue to permeate all aspects of our lives.

So, why go to all the effort to ensure CDs are secure and we have the processes in place to support and maintain that security? Let's start with the death of diesel.

MARKET DRIVERS

The diesel car is on its death bed with the UK government stating that new exclusive diesel and petrol cars will be banned in 2040.[1] The time of the electric vehicle is here; and with it comes the task of installing an infrastructure capable of supporting them. It is estimated that the additional peak demand due to electric vehicles is likely to reach 18GWs by 2050.[2] This, in combination with the increased use of energy from renewable sources, and the developments in battery storage all define the need for a Smart Grid, i.e. an infrastructure facilitating better integration of microgeneration and renewable technologies, lower maintenance costs, and most importantly, better matching of supply and demand.

There is also evidence of Smart Grid technology interacting within CDs in the domestic market via Smart Meters (and associated equipment such as Consumer Access Devices[3]) in the government consultation on the regulation of Smart Appliances.[4] Allowing domestic appliances to interact with the Smart grid to provide Demand Side Response (DSR) to facilitate load balancing.

A smart grid cannot be realised without secure CDs and services to monitor, analyse and react to changes in demand.

Further drivers are emerging from the water industry, where increasing city populations and finite resources have resulted in use cases being proposed to monitor and diagnose leakage to improve maintenance of the water infrastructure and drive efficiency[5], all realised using CDs.

[1] https://www.gov.uk/government/news/plan-for-roadside-no2-concentrations-published

[2] http://fes.nationalgrid.com/media/1253/final-fes-2017-updated-interactive-pdf-44-amended.pdf

[3] http://www.beama.org.uk/resourceLibrary/consumer-access-devices-a-beama-guide.html

[4] https://www.gov.uk/government/consultations/proposals-regarding-setting-standards-for-smart-appliances

[5] https://utilityweek.co.uk/pr19-prime-opportunity-water-sector-drive-efficiency/

In fact, use cases for CDs are being proposed across nearly all market verticals, including manufacturing[6], transportation[7] and social care[8] to name but a few.

Add to this the sheer number of technology incubators and accelerators, both government and privately funded, encouraging the development of products and services provides further indication that CDs are here to stay (unlike the originals); and therefore, the time has come to address how we will securely manage them today, and in the future.

Next, we will look at some of the recent regulations around security and data privacy that will impact CDs.

REGULATION

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR focuses on the right to privacy of individuals and states "*The controller shall...implement appropriate technical and organisational measures...in an effective way... in order to meet the requirements of this Regulation and protect the rights of data subjects*".[9] Whilst GDPR primarily focusses on data privacy, there is no privacy without security and therefore, if CDs collect, store or process personal data they are required to implement appropriate security measures to protect that data.

The point could be made that if data is worth collecting it is valuable and therefore non-personal data should be protected in an equivalent manner. For example, taking the previous example of a temperature sensor in an industrial greenhouse, the confidentiality (privacy) of this data is not very important however the integrity of the data collected is fundamental to the operation of the service.

NETWORK NFORMATION SYSTEMS (NIS) DIRECTIVE

The NIS directive has been somewhat eclipsed by GDPR and focusses more on cyber security and resilience of essential services. It states "One of the key objectives of the NIS Directive is to ensure that Operators of Essential Services (OES) take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which support the delivery of essential services".[10]

Once again if CDs are deployed as part of an essential service then appropriate security measures must be in place.

[6] https://www.ioti.com/industrial-iot-iiot/top-20-industrial-iot-applications

[7] https://enterpriseiotinsights.com/20180126/transportation/three-smart-transportation-case-studies-tag17-tag99

[8] https://iotuk.org.uk/iot-in-health-and-social-care-report/

[9] https://www.eugdpr.org/the-regulation.html

[10] https://www.ncsc.gov.uk/guidance/introduction-nis-directive

SECURE BY DESIGN

The “Secure by Design” initiative is a code of practice rather than a regulation (at this time) and it addresses the “low hanging fruit” to secure IoT devices, stating “Poorly secured devices threaten individuals’ online security, privacy, safety, and could be exploited as part of large-scale cyber-attacks”.[11] It lists 13 key security principles, that should be observed when developing CDs and is considered a minimum baseline.

We have market drivers that indicate that there is a need for CDs and the services they can provide; and we have regulations and codes of practice that state we should take “appropriate” technical measures to protect them. The big question is “How”. In the next section we will look at some of the changes to our security processes that will need to be made to address the use of CDs.

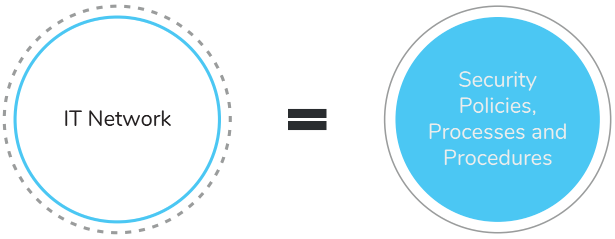
WHAT IS APPROPRIATE?

Both GDPR and the NIS Directive state that “appropriate technical and organisational measures” must be in place to ensure data privacy and security. As stated earlier the term CD covers a vast range of devices, functions and capabilities and therefore a one size fits all approach is not possible, therefore appropriate security must be defined based on the risk profile of the device. Which in turn must consider the data it handles, its function within the network, its operational environment and the potential impact to the wider network when it is breached (always use a “when, rather than if” approach to security), however as stated previously, the DCMS “Secure by Design” principles should be considered the ***minimum*** security baseline for CDs.

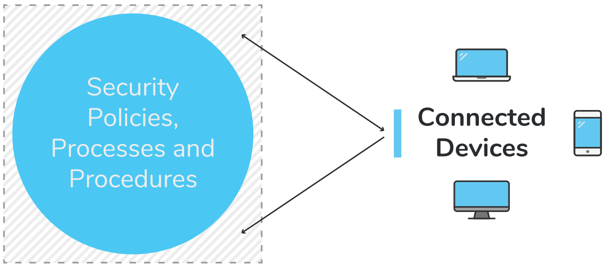
As CDs become more prevalent in our day to day lives it is important to ensure our processes evolve to maintain the security of the services they offer, in a comparable manner to the way that our processes changed in light of the increased use of mobile devices. There is very little difference at the network level between a standard IT device (such as a laptop or desktop) and a CD, however there are some key differences that must be considered.

DON’T REINVENT THE WHEEL

Existing IT security processes provide a starting point to address the inclusion of CDs. Imagine an IT network represented as a circle, we can create a set of processes to provide coverage across the network.



However, as CDs are added to the network (represented as a square rather than a circle), we may find that our IT security processes no longer cover all aspects, leaving CDs in the shadows.



We should be looking to update our processes to shine a light into the shadows of the network to ensure we address the ***entire*** network. We will look at some additional areas of consideration, related to CDs, in the following sections.

[11] https://www.gov.uk/government/news/new-measures-to-boost-cyber-security-in-millions-of-internet-connected-devices

PROCUREMENT

Before procuring CDs ensure that the business use case is understood, and the associated risks have been identified, analysed and translated into the procurement process. At the very least any device should meet the basic requirements of the Secure by Design code of practice and, where applicable, maintains a security characteristic appropriate to the identified risks.

To support this, suppliers of CDs should be able to provide basic information regarding the devices security characteristic, its suitability to operate within regulated frameworks such as GDPR and NIS and; how long they will provide support for such devices. If businesses start to ask the questions, suppliers will be required to provide the answers.

INSTALLATION AND CONFIGURATION

Who is responsible for installing, configuring the CD? An internet connected thermostat could be installed by a facilities department, but as it is connected to the network, the IT department must also be aware of it. Therefore, coordination between internal departments must be in place to ensure that security is maintained. This becomes even more relevant if the CD has a high-risk profile or collects personal data, such as an internet connected camera. Similar process will have to be in place when the CD is decommissioned and removed from the network.

ASSET MANAGEMENT

The scale of CDs brings additional challenges around asset management, the number of devices in a network could be thousands, hundreds of thousands, or even millions. Understanding what devices are on your network and successfully managing them throughout their lifetime will require a co-ordinated set of business processes and technical controls, spanning both internal departments and external organisations.

IN-LIFE MAINTENANCE

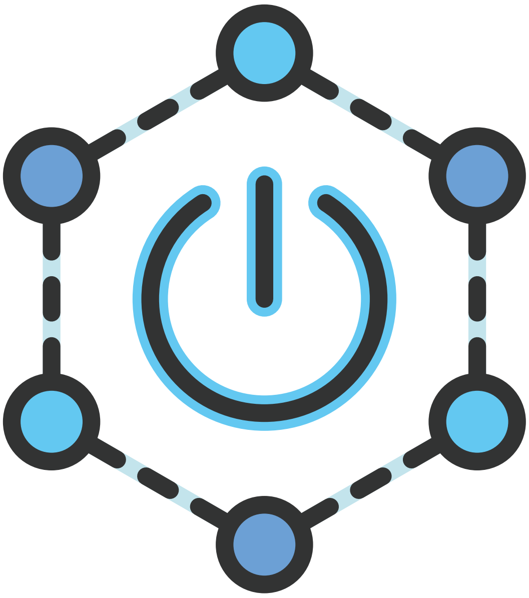
Include processes to address who is responsible for maintaining the security of device, both internally and externally, i.e. will the manufacturer keep the device updated, or will the service provider be responsible for this role? The relationship between manufacturer and service provider is likely to be closer than when managing traditional IT systems as the root of trust for a CD tends to start on the manufacturing line. It is important that our processes understand this and include prerequisites around secure manufacture and logistics, developing a "supply chain of trust".[12] Service operators should consider including CDs in the scope of any periodic security assessments whether internal or external such as ISO 27001.

It is also important that there are channels of communication open between suppliers, service operators and security researchers to ensure that vulnerabilities are reported, assessed and rectified in a timely manner.

IN CONCLUSION

There are significant real-world problems that can be addressed using CDs. There are market drivers in place to define the need and regulatory drivers to ensure data privacy and security. We therefore need to be able to manage these systems throughout their lifetime to ensure the confidentiality, integrity and availability of CDs and the services they support. We also need to foster greater coordination between manufacturers, operators and security professionals to ensure security is addressed across the supply chain and throughout the life of a device.

GDPR and NIS provide us with an opportunity to develop a robust set of process to maintain a secure network of CDs and services that will help ensure a solid foundation for the IoT and build a strong digital economy.



[12] http://www.newelectronics.co.uk/article-images/152099/P18-19.pdf

Author

Sean Gulliford
Principal Consultant

Contact Us

To get in touch with us contact us at:

E: bd@gemserv.com
T: +44 (0)20 7090 1091
W: www.gemserv.com
@gemservinfosec

London Office
8 Fenchurch Place
London
EC3M 4AJ

Ireland Office
Fitzwilliam Hall Business Centre
Fitzwilliam Place,
Dublin 2

Company Reg. No: 4419878