THREE INDISPENSABLE ELEMENTS OF IOT SECURITY

Viakoo

Copyright Viakoo ©2020

(650) 263-8225 | sales@viakoo.com | viakoo.com

This paper explains why Enterprise IoT systems will not be cyber secure until three critical elements of their device security are made manageable at scale. It also describes how to do that.

Enterprise IoT

The **Internet of Things** (IoT) refers to smart devices that connect to the Internet for purposes of data exchange, remote monitoring, or control. Typically, these are **personal and residential consumer** devices. Likewise, the **Enterprise Internet of Things** refers to networked IoT devices that are used for business and industrial data exchange, remote monitoring, or control.

Consumer IoT devices are few per person and deployed individually or in very small systems. In contrast, Enterprise IoT devices are numerous and deployed in very large scale systems. Many of them are intelligent devices, and except for being purpose-built devices or appliances, could rightfully be called "servers", because they contain processors, memory, storage and networking, along with web interfaces for human configuration and application programming interfaces (APIs) for streaming

> *Large organizations with deployments of IoT security cameras, DVRs, and sensors will be especially impacted by ransomware's pivot from the desktop to IoT.*
>
> **CALEB BARLOW**

(serving) data out to one or more systems and applications. Other IoT devices, also intelligent and purpose-built, perform control functions using one or more specific control message protocols. IoT devices are key components of a larger system managed by software applications. For the purpose of this paper, we will refer to them as unmanaged or distributed IoT devices.

The characteristics of such IoT devices make them easy and attractive targets for manual and automated cyber-attacks.

IOT PROVIDES EASY CYBER TARGETS

There are over a dozen reasons why **distributed IoT** devices are attractive targets for hackers:

1. **Critical Functionality.** ome devices, like traffic lights, perform critical functions which can significantly impact the system they are part of if their operation is compromised. For malicious individuals, the chance to cause device malfunction and wreak havoc – especially in a newsworthy fashion – is attractive.
2. **Appropriable Processing Power.** Obtaining root or admin access to an intelligent device makes it possible to appropriate some of its processing power to run malicious software (malware) and perform the bidding of the hacker, especially acting as a "robot" or "bot" at the direction of a hacker's command and control server. Video requires a significant amount of processing power compared to text processing, thus the processing needed to run malware is just a fraction of a security camera's overall capacity.
3. **Scale.** There are several scale factors that make IoT devices attractive. Thousands, hundreds of thousands, and millions of devices can be compromised and connected to a hacker's command and control server. This happened in 2016 when 1.5 million connected cameras and recorders were hijacked to make the world's largest botnet (Fenceschi-Biccheria, 2016). What's more, most distribute IoT deployments aren't manageable at scale given the lack of tools designed to operate at that scale. When hackers have scalable tools and undetectable approaches, and IoT systems are maintained via manual tasks, hackers can easily remain in control of captured devices.
4. **Doorway.** Even a small network of Enterprise IoT devices is usually connected to a larger network, and so compromising a single device can act as a doorway to other critical targets.

5. **Always On.** IoT devices run 24/7 all year round in networked infrastructure that is out of site of the users of the IoT systems the devices belong to. Thus, their attack surfaces are always available and visible to attackers, but the attacks are not visible to system users.
6. **Stripped-down OS.** They often run on the Linux operating system—but use an embedded or stripped-down version that is relatively easy to infect with malware.
7. **Common Outdated Code Libraries.** Many devices include widely used common low- or no-cost code libraries that are often outdated and contain vulnerabilities.
8. **Lack of Basic Security.** IoT devices generally don't have enough processing power to run security applications like servers and workstations do. This means they don't detect and thus can't block or even report malware infections. Device infections can last for years without device owners becoming aware of them.
9. **Password Weaknesses.** Most intelligent IoT devices use default passwords like admin, system and password. Default passwords are commonly published online in installation guides and thus available to all users and hackers alike. Most in-house and contracted installing and servicing technicians use the same rememberable Admin level password or password scheme across all IoT devices. Contractors sometimes proliferate them across multiple customers. Many end users use common and easily-guessable passwords.
10. **Third Party Services.** Most Enterprise IoT devices are part of systems that are installed or maintained by third-party services, whose personnel typically have poor password management practices and keep them in obviously-named spreadsheets or text files, and whose networks are often less secure than those of the companies they service. This was the case with the infamous Target data breach of 2013, in which information for as many as 70 million credit card accounts was stolen, by hackers using network access credentials stolen from their HVAC service contractor. (Krebs, 2014a, McGrath, 2014).

11. **Outdated Firmware.** Most IoT devices rarely have their firmware updated due to the inconvenience of manual update processes, and the lack of tools for automating such updates. As a result, even though manufacturers correct firmware vulnerabilities and issue new firmware, many device owners have a practice of not performing updates and yet at the same time can't detect when their devices have become compromised. Firmware has the highest device privileges, allowing attackers to bypass traditional controls and gain persistent access to device functionality undetected.

12. **Weak Authentication.** Authentication refers to the process of proving an identity to an application or system – in other words, demonstrating that you are who you say you are. Affinity IT Security defines Weak Authentication as "any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected," including "scenarios in which the authentication mechanism is flawed or vulnerable." (Affinity IT Security 2020) In most IoT devices, this means providing a name and password. Manual name and password management for multiple users and hundreds or thousands of devices is a daunting task. That is why users and technicians use workarounds, such as shared passwords and reusing passwords across multiple devices. It's also why such passwords are rarely changed.

13. **Lack of Strong End-to-End Encryption.** When data is transmitted or stored in plain text, unauthorized access to the data becomes a breach of confidentiality, and potentially a breach of data integrity if the data is changed. System-wide use of strong data encryption ensures that if the data is accessed it can't be made sense of, and if changed in a data stream or a data record, the fact of that change is evident. Most IoT deployments have little to no encryption of their data, which means that if unauthorized data access is achieved then confidentiality, integrity and availability can be lost.

14. **Malware Designed for Specific Devices.** Malware exists that was designed for specific IIoT device makes, models, and embedded OS and code libraries, so the malware can perform its intended task without compromising the functionality of the device, until the hacker decides to do take the device over or cripple it.

> *SonicWall discovered several variants of Mirai that were re-tooled to add new vulnerabilities or target specific devices.*
>
> **2018 SONICWALL**

These characteristics make IoT systems high-value cyber targets, because they are easier to compromise than other types of systems, and many such compromises are likely to go undetected. The fact that IoT devices are unattended (rarely have user interaction) means that many types of device compromises will go unnoticed. Especially when the malware is designed not to disrupt the device's primary functionality.

This is why, regarding the large 2016 Mirai botnet attacks, it's so hard to nail down the number of compromised devices, and why the estimates range from 600,000 to 1.5 million devices. The majority of those devices were security video cameras and digital video recorders, many of whose owners still have no idea that their devices had been compromised and were being used to perform massive cyberattacks.

Mirai used common factory default usernames and passwords to gain access to connected devices and infect them with malicious code. SonicWall discovered several variants of Mirai that were re-tooled to add new vulnerabilities or target specific devices. (SonicWall, 2018)

ATTACK SURFACES, ATTACK VECTORS

An intelligent device's attack surface consists of all the ways that an attacker can attempt to gain unauthorized access to the device for nefarious purposes, including to steal information, disable one or more device functions, secretly use a device's computing power, and control a device for harmful purposes. An attack vector is the path by which a live hacker or malware can gain access to the device.

Password weaknesses (typically name and password pair) and firmware vulnerabilities are the two most common attack vectors

for IoT devices. Unencrypted or weakly encrypted input and output data are sources of data that human hackers can use to find other means of gaining device access and causing harm.

The nature of these attack surface vulnerabilities involves class breaks, where the compromise of a single device enables access to an entire group of devices. This also allows simultaneous access to a large set of devices all at once, usually because there is no warning or alert about the initial compromise, but also because there is not enough time after the first compromise for the rest of the devices to have their passwords changed manually. This has to occur in both the device itself, and in any system using the password to establish a connection to the device.

> *Attackers examine our systems, looking for class breaks. And once one of them finds one, they'll exploit it again and again until the vulnerability is fixed.*
>
> **BRUCE SCHNEIER**

Bruce Schneier, an American cryptographer and computer security professional, elaborates (Schneier, 2017). "In a sense, class breaks are not a new concept in risk management. It's the difference between home burglaries and fires, which happen occasionally to different houses in a neighborhood over the course of the year, and floods and earthquakes, which either happen to everyone in the neighborhood or no one. Insurance companies can handle both types of risk, but they are inherently different. The increasing computerization of everything is moving us from a burglary/fire risk model to a flood/earthquake model, which a given threat either affects everyone in town or doesn't happen at all.

"But there's a key difference between floods/earthquakes and class breaks in computer systems: the former are random natural phenomena, while the latter is human-directed. Floods don't change their behavior to maximize their damage based on the types of defenses we build. Attackers do that to computer systems.

Attackers examine our systems, looking for class breaks. And once one of them finds one, they'll exploit it again and again until the vulnerability is fixed."

Furthermore, an attacker who is an insider is often able to hide an attack that would otherwise be more discoverable when performed from the outside.

Additionally, lack of device authentication allows rogue (i.e. unauthorized) devices to connect to a network and secretly read network traffic to capture logon credentials and other information. Rogue devices may also relay and possibly alter communications between two devices that are unable to detect that they are not directly communicating with each other, commonly called a man-in-the-middle (MITM) attack.

Protecting IoT Devices

Protecting a distributed IoT device involves reducing the device's attack surface by eliminating or hardening points of attack, especially for three areas of vulnerability where compromises can result in class breaks:

- Logon credentials
- Firmware vulnerabilities
- Digital certificates used for device ID and data encryption

The ongoing application of good cyber security practices is commonly referred to as cyber hygiene.

LOGON CREDENTIALS

Logon credentials, such as for security video cameras, are especially vulnerable in high device count deployments because

it's hard to conform to good password practices; manual password management just doesn't scale up. Typical poor password practices include sharing passwords across large groups of devices; service personnel use of "favorite" passwords across different customer deployments; and delegation of password management to service firm technicians servicing device groups.

These practices create class break vulnerabilities, where the compromise of a single device's logon credentials enable access to the entire group of devices. It also allows simultaneous access to large sets of devices all at once.

Automated tools can be used to ensure that default passwords and easily-guessed passwords are not used. Hackers use some of them to find devices they can compromise. Secure (i.e. HTTPS) network connections can be used to ensure that passwords are not transmitted in plain text. Some IIoT device vendors offer software for managing passwords, but most require manual processes and are not feasible to use on large scale systems.

Ideally, to harden device logons, an automated password management application would be used to:

- Assign unique names and passwords to each individual device, updating the passwords in the system applications that use the devices, eliminating the class break vulnerability.
- Provide a single sign-on capability so that human users require just one set of logon credentials to access any device, which would be enabled as-needed for short periods of time and be cancelled when user authorization ends.
- Allow system-level manual means of changing device passwords to be disabled, minimizing insider risk.
- Implement password management strategies such as automatically changing passwords every 30 days and using strong passwords.

Additionally, name and password credentials should never be transmitted in the clear but should always be send via an encrypted means of communication. For on-premises IoT devices, the time

needed for an attacker to compromise a device can be very high. However, if the attacker is able to steal the logon credentials, that time is significantly reduced.

FIRMWARE VULNERABILITIES

By 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability (Harvey, 2019). Analysis of ransomware distribution methods implicated compromised firmware as the 3rd most common infection vector in the first half of 2019 (Michael, 2019). The number of attack events measured during that period was twelve times higher when compared with the same period in 2018, an increase largely ddriven by IoT-related traffic. The detected malware was dominated by various versions of Mirai, which is still going strong three years after it first burst onto the scene in 2016 (Michael, 2019).

> *By 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability.*
>
> **GARTNER**

Mirai targets IoT devices such as IP cameras and routers, infects those using default credentials, and co-opts them into botnet armies. In a new trend that should concern every business, Mirai has recently spawned variants that are specifically engineered to infect enterprise IoT devices such as wireless presentation systems and digital signage TVs (Michael, 2019).

This means that business local LAN and core networks are being targeted and will constitute an active attack vector for IoT systems connect that connect to a business network to share or obtain data.

Some cyber liability insurance policies have exclusions that disqualify insurance claims from businesses whose attack entry point or means of spreading was an industrial or building control system (including a security system), especially if the system doesn't have a documented cyber hygiene program in place. This is another reason why IoT device firmware vulnerabilities warrant greater concern than is typically given to them.

For all the above reasons, intelligent IoT device cyber hygiene must incorporate sound firmware management, including these practices:

- Maintain documentation of device firmware versions that includes a cross-reference matrix documenting the firmware version support of each version of application residing on or using the devices.
- Maintain an inventory of device firmware and application software that have been tested and approved for deployment, with digital signatures for the firmware and application files to verify their authenticity and ensure that they haven't been tampered with since they were verified.
- Establish the ability to quickly update device firmware as new firmware versions are released.
- Monitor vendor device security web pages, and subscribe to vendor security notices, to be aware of when new security issues are found, and corrective firmware releases are issued.
- Maintain a log of when firmware updates were performed and by whom for verification of compliance to security policies and practices.

Note that security fixes are not always documented in firmware release notes, which means that each firmware update, even if supposedly containing only feature updates, must be applied to be assured that all security issues known to the manufacturer have been corrected in your device deployment.

DIGITAL CERTIFICATES

Public key encryption, which is based on digital certificates, is the strongest known form of encryption. This is why it is increasingly being used in IoT for encrypting important data exchanges. Digital certificates are produced by public key infrastructure (PKI), which is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. In a network-based distributed IoT system, such as a security video surveillance system, digital certificates are used for:

- Identification. Which specific device, computer or application is this?
- Authentication. Can we trust that it's not an impostor?
- Secure exchange of encryption keys. What encryption key shall we use to encrypt the data stream?

Digital certificates and the encryption keys they contain are used to enable features such as device identification and authentication, HTTPS computer and device connections, secure network monitoring, IEEE 802.1x network access control, and secure streaming media transmissions.

IoT is becoming a major driver for the use of PKI. There is growing recognition that PKI provides important core authentication technology for the IoT. The Ponemon Institute conducts an annual survey about PKI deployment. The survey results include the number of respondents who say that IoT is the most important trend driving the deployment of applications using PKI. That number has increased significantly from 21 percent of respondents in 2015 to 41 percent in 2019 (Ponemon, 2019).

Leading manufacturers of IoT intelligent devices are starting to provide strong support for the use of digital certificates that is in line with current-day certificate management practices. For example, network video cameras from Axis Communications support

certificate-based Secure Real-time Transport Protocol (SRTP). Axis camera SRTP implementations with its video management system partners such as Genetec (Axis & Genetec, 2018) and Milestone Systems change the video streaming encryption keys (securely derived from an exchanged master key) as frequently as every 60 seconds, to ensure that no single block of encryption is large enough to facilitate certain types of attacks against the encrypted data.

CERTIFICATE ROTATION

Certificate rotation is the replacement of existing certificates with new ones. Replacement is required when a certificate is expiring, when the certificate chain of trust has been compromised, or when the contents of one or more certificates must be changed.

Digital certificates should be set to expire at intervals that make sense based on their use. If a certificate has been compromised without discovery, expiration shortens the length of time that the compromise can be used to advantage by an attacker. For most IoT devices that stream data continuously 24/7, a monthly interruption for less than a minute for certificate replacement is an acceptable data stream interruption given the security value of the certificate change, especially if the data is buffered. Many organizations rotate their certificates at more frequent intervals than their expiration periods.

For large scale intelligent device deployments, automated certificate management is necessary. Manual rotation of digital certificates for hundreds or thousands of devices is not only costly and wasteful of resources, but error prone. Thus, to date, as has been the case with IoT firmware updates, IoT device certificate replacements are

seldom or rare and digital certificate life has typically been set to as many as 5, 10 or 20 years. Long certificate lives are commonly used where automated certificate management has not been established and where those responsible for device management are unaware of the increasing security threats against certificates. They are also common for devices that are shipped with or generate self-signed certificates, which are more vulnerable than certificates issued by a trusted independent certificate authority (CA).

DEVICE MANAGEMENT AT SCALE

In previous decades, the predecessors to today's IoT devices were not intelligent devices and typically provided sensor data for a small closed system. Street intersection traffic lights, for example, operated on independent schedules. The devices were not hacker targets since they weren't part of a larger network and could only be accessed by hands-on presence. Such devices only needed defense against physical attacks. There was no need for large-scale device management.

Today's intelligent IoT devices are often part of large-scale networks, such as city traffic management systems. For all the reasons listed at the start of this article, IoT devices are attractive to hackers, who have software tools to attack devices at a large scale and put thousands of them under the direction of a single command and control server. It is a sad and risky situation that attackers have better tools to manage IoT devices at scale than the device owners do.

In 2018 Caleb Barlow, then IBM Security's Vice President – Threat Intelligence, said, "We suspect next year we'll start to see larger scale attacks in the IoT space. System administrators need to understand the inventory of where these IoT devices are located, what they are connected to, and how to update them. Further, regarding any IoT device, Barlow said, "We need a way to update it in real time over the wire, and if we don't have that we should really question why we should use it [the IoT device]." (Brown, 2018).

TIMELY DEVICE DEFENSE

Effective response to a discovered, or credible threat of, device compromise is to quickly and securely perform the first two or all three actions:

1. Change all logon credentials
2. Update all firmware that's not the most recent version
3. Change all digital certificates (if any certificates or certificate issuers have been compromised)

Often this requires updating the software that interacts with the devices.

Manual updating of large device count deployments can take weeks or months, which is ineffective for an attack that's imminent or already under way. This is why automated tools are required that span the breadth of an IoT deployment and can concurrently update large numbers of devices in parallel on demand.

MEAN TIME TO HARDENING

Richard Melick, Sr. Technical Product Manager for Automox, suggests a new security metric: Mean Time to Hardening (Melick, 2019). It is the time between the disclosure of a product vulnerability and the hardening of the deployed product to address the vulnerability. Melick explains, "Given that the average time to weaponization is seven days, with many weaponizations released inside of that window like the infamous Apache Struts vulnerability that took down Equifax, you effectively have 72 hours to harden your systems before you should expect to see new exploit techniques surface. When zero-days occur, the best-in-class response window is within 24 hours of disclosure. While this 24-hour threshold is ambitious, it's the pace you'd need to move to realize a pre-incursion defensive effect."

Given the increasingly more capable threat landscape, the key security objective should be radically reducing device vulnerability exposure time, hence the metric, Mean Time to Hardening (MTTH).

Melick further cautions, "To achieve a defensible outcome, organizations need to focus on the velocity in endpoint hardening. And that's why the 24/72 MTTH threshold is the next benchmark organizations need to achieve, testing and rolling out mitigations in an accelerated, yet methodical manner."

DEVICE DEFENSIBILITY AT SCALE

For large device-count IIoT deployments, maintaining an up-to-date device security profile and responding quickly to device attacks requires automated device management at scale. That includes automated management of logon credentials, firmware updates and certificate rotation.

The driver behind security hygiene is that there are a relatively small number of root causes for many data breaches, malware infections, and other security incidents. Implementing a few relatively simple practices can address those root causes to prevent many incidents from occurring and to lower the potential impact of incidents that still occur. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause (Souppaya et al., 2018).

Key Steps to Full Device Defensibility

Take the following steps to determine where you stand regarding your distributed IoT device defensibility. Each step is referenced to the CIS Controls® listed in the Version 7.1 CIS Controls Internet of Things Companion Guide (CIS, 2019). Note that the step numbering is independent of the CIS control numbers.

1. **Hardware Inventory.** Update (or create) your inventory of IoT devices and the applications that that utilize them. Also include the servers on the network to which the device connects. (CIS Control 1)

    1.1. **Documentation.** Identify each device and document:

        1.1.1. **Device Information.** MAC address, IP address, make and model, current firmware version, latest available firmware version.

        1.1.2. **Dependencies.** List the applications and other devices having data interface compatibility dependencies on the firmware version of the device being inventoried and documented. Inventory the software application in step 2.

1.1.3. **Security Information.** Is 802.1x network access control supported and if so, in use? Are the device/server client certificates self-signed or CA-issued, and what is the certificate expiration date?

1.1.4. **Product Life Cycle.** Purchase date, warranty expiration date, end-of-sales and end-of-support dates; organization's asset owner; other organization-relevant life cycle information.

1.1.5. **Monitoring.** Is SNMP or other device monitoring in use? If so, note or reference details.

2. **Software Inventory.** Update (or create) your inventory of software applications that interface with or are dependent on data from one or more IIoT devices. (CIS Control 2)

2.1. **Documentation.** For each application:

2.1.1. **Software Information.** Software vendor, current software version, latest available software version.

2.1.2. **Dependencies.** Cross reference the hardware inventory to identify the devices with which the application has data interface compatibility dependencies on the firmware version of the device, and software version details specific versions require specific device firmware.

2.1.3. **Security Information.** Does the application vendor provide deployment hardening advice? Has it been applied? Have the server and operating system been hardened per manufacturer's advice?

2.1.4. **Product Life Cycle.** Purchase date, warranty expiration date, end-of-sales and end-of-support dates; organization's asset owner; other organization-relevant life cycle information.

3. **Continuous Vulnerability Management.** If continuous vulnerability management is not yet in place for the IIoT devices and applications, for each type of device and application, determine how to continuously acquire, assess, and act on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. (CIS Control 3)

3.1. **Tools.** For each type of IoT device:

3.1.1. **Qualify.** Identify the automated tools that are most suitable for managing at scale device passwords, firmware updates, and certificate management. Remember that the tool must update the logon credentials not only in the devices, but also in the software and other devices that use the logon credentials to

authenticate themselves. Automated credential management must use the dual-certificate or another approach to minimize offline time required for certificate rotation in devices and applications.

3.1.2. **Cost.** Determine the tool costs and cost options.

3.1.3. **Select.** Identify the tools that most closely fit the IIoT deployments security needs.

3.2. **Implementation Approach.** If the organization has another vulnerability management program or process exists, align with or enroll in that program or process as appropriate.

3.3. **Remediation.** Outline a risk-rating process to prioritize the remediation of discovered vulnerabilities.

3.4. **Roles and Responsibilities.** Determine the roles required for vulnerability management and identify candidate in-house or service-provider personnel for them.

3.5. **Levels of Effort.** Determine the internal level of effort required to implement full IoT device defensibility. If outside resources are needed, determine their level of service required and its cost.

4. **Incident Response.** Consult with any existing technology infrastructure response team to understand the incident response coordination required regarding updates to IoT device logon credentials, firmware and certificates if that will be part of a larger response effort. If not required, then outline a simple incident response plan. (CIS Control 19)

5. **Planning and Approval.** Develop an outline plan for implementation. Collaborate with resource approval (funding and collaborative resources) and other organization stakeholders to finalize the plan for approval.

5.1. **Outline Plan.** Develop a budgeting approach and an outline plan for implementing the device defensibility capabilities once the budget is approved.

5.2. **Stakeholders.** Consult with internal stakeholders who have an interest in the benefits of the improved IIoT security profile that will result. Obtain their support as appropriate.

5.3. **Approval.** Request and obtain approval for the IoT device security profile improvements.

Conclusion

High device count distributed IoT systems are now valued cyber targets because they currently have poor to no cyber hygiene and are easy to secretly compromise at scale. Fortunately, leading device manufacturers are improving device cybersecurity features, and some have begun facilitating device management at scale.

Take the five steps above to harden your enterprise IoT attack surfaces and achieve a highly defensible deployment.

About Viakoo

Viakoo (viakoo.com) ddelivers performance, security and compliance management for Enterprise IoT Applications and Devices. Video cameras, access control systems, intercoms, and other IoT systems typically are managed piecemeal or manually. Viakoo's SaaS offering automates the verification of these heterogeneous systems to confirm they are working properly and are secure from end-to-end

Viakoo's 500+ million hours of experience with 100s of applications and 1000s of device types ensures Enterprise IoT applications are available, performant and secure 24×7. Enterprises see value from Viakoo in minutes as Viakoo detects configurations automatically.

Viakoo is located in Mountain View, California.

Copyright Viakoo ©2020

Bibliography

Affinity IT Security (2017). Article: What is Weak Authentication? Affinity IT Security. [online] Available at: https://affinity-it-security.com/what-is-weak-authentication/ [Accessed 7 Mar. 2020].

Axis & Genetec (2018). EBook: Encrypting network streams: An overview of why and how to encrypt network video. Genetec, Inc. Available at: https://info.genetec.com/axis-genetec-ebook.html.

Brown, Leah (2018). Article: Ransomware attacks will target more IoT devices in 2018. [online] Available at: https://www.techrepublic.com/article/ransomware-attacks-will-target-more-iot-devices-in-2018/ [Accessed 14 Apr. 2020].

Fenceschi-Biccheria, Lorenzo (2016). Article: How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet. [online] Motherboard.com. Available at: https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs [Accessed 15 Jan. 2020].

Harvey, Tony (2019). Report: How To Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds. Gartner. (Gartner subscription required)

Krebs, Brian. (2014). Article: Target Hackers Broke in Via HVAC Company — Krebs on Security. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ [Accessed 7 Mar. 2020].

Krebs, Brian. (2014). Article: Inside Target Corp., Days After 2013 Breach. Krebs on Security. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/tag/fazio-mechanical/ [Accessed 7 Mar. 2020].

McGrath, Maggie. (2014). Article: Target Data Breach Spilled Info On As Many As 70 Million Customers. [online] Forbes. Available at: https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#7d956224e795 [Accessed 7 Mar. 2020].

Melick, Richard. (2019). Article: Mean Time to Hardening: The Next-Gen Security Metric. [online] Threatpost.com. Available at: https://threatpost.com/mean-time-hardening-next-gen-security-metric/151402/ [Accessed 7 Mar. 2020].

Michael, Melissa (2019). Article: Attack Landscape H1 2019: Iot, SMB Traffic Abound - F-Secure Blog. [online] F-Secure Blog. Available at: <https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/> [Accessed 7 April 2020].

Ponemon Institute (2019). Report: 2019 Global PKI and IoT Trends Study. Ponemon Institute. Available at: https://www.ncipher.com/2019/pki-iot-trends-study/

Schneier, Bruce (2017). Article: Class Breaks. Edge Foundation, Inc. [online] Available at: https://www.edge.org/response-detail/27068 [Accessed 7 Mar. 2020].

SonicWall, (2018). Report: 2018 SonicWall Cyber Threat Report. Available at: https://cdn.sonicwall.com/sonicwall.com/media/pdfs/resources/2018-snwl-cyber-threat-report.pdf

Yang, Mary et al. (2015). Guide: CIS Controls Internet of Things Companion Guide. Center for Internet Security, Inc. Available at: https://www.cisecurity.org/white-papers/cis-controls-internet-of-things-companion-guide/