How can small to medium businesses adopt IoT devices and still stay secure.

Abstract

As time passes, along with external factors such as the Covid-19 pandemic, IoT devices are being further and further integrated into both the lives of individuals and the running of businesses. This trend is only going to increase over the coming years, along with the need for devices and systems to be more efficient and easy to use for the masses. This paper will address IoT device security flaws and how they could leave the businesses that use them at risk of attack, ethical considerations to be made when implementing IoT devices, and how best to implement them with a focus on security.

1. Introduction

An IoT device is a device that collects contextual data using sensors to either action it or send it on to another connected device to perform an action (Hossain et al, 2015).

IoT solutions provide a huge amount of convenience for the end user, making automation of mundane tasks in all sectors of life and work much easier. It is due to these easy to obtain results that IoT adoption has seen staggering growth in the last decade. As can be seen in Figure 1 below the number of IoT devices is predicted to out number non-IoT devices 3:1 in the year 2025. This growth will bring new innovation along with inevitable new security vulnerabilities and risks.

Figure 1. A graph of connected devices split between IoT and non-IoT devices from 2019-2025 (Lueth, 2020).

As we progress through the century niche technology such as augmented and virtual reality will continue to be developed and refined, eventually being integrated with the smart devices surrounding us now. Businesses that consider their IoT security in detail now will be able to carry over or modify their existing solutions for emerging tech.

2. Types of IoT

Depending on the type of business being ran, the IoT devices being used can vary significantly along with the security issues that they bring with them.

2.1 Industrial IoT

Industrial IoT or IIoT refers to the application of IoT connected devices in industrial applications such as manufacturing, assembly and logistics (Trend Micro, n.d). The implementation of these is often referred to as "Industry 4.0". While adoption of IoT technology can improve productivity by 10-25% (Ezell, 2016), cyber security failures in industrial processes such as these can have some of the most expensive and dangerous consequences. For example the first cyber "weapon" deployed by a nation state Stuxnet targeted industrial control systems in an Iranian uranium enriching plant, causing centrifuges to self destruct by spinning them up well beyond their recommended speeds. This shows us that consequences of IIoT attacks can range from a simple data leak to multi-million pounds worth of damage to physical systems too.

2.2 Consumer Devices

Consumer IoT devices have seen massive growth in the past few years with smart assistants such as Amazon's Alexa and wearables like smartwatches and other personal monitors. This trend is only predicted to increase as can be seen in figure 2 below with WPAN (Wireless Personal Area Network) devices set to hit 8 billion devices by 2025, the same number as all of the IoT devices only 7 years previous.

Figure 2. A breakdown of the different IoT device types from 2019-2025 (Sinha, 2021).

Much like IIoT is driving the creation of "Smart Factories" the consumer market for IoT is driving the creation of "Smart Homes". These two phenomena have the same goal of increasing efficiency and usability. Households in the United States had an average of 11 "smart" devices in 2019 (Westcott et al.), compared with 25 in 2020 (Brassfield). That's a 227% increase in just a single year, if this trend continues US households could contain on average hundreds of connected devices by 2025. The side effect of adding more and more devices to the household is creating a much larger attack surface. The increased demand could also drive prices down possibly forcing manufactures to spend less on security to keep up with the market.

Medical IoT

Medical smart devices offer a lot in terms of quick availability of medical information for patients and healthcare professionals. For example an individual with diabetes can use a device called a Continuous Glucose Monitor, this is a small device that sits under the skin and gives instant read outs of glucose levels and alerts the user to dangerous blood sugar levels (Diabetes UK, n.d). This device uses Bluetooth to communicate and an attacker could feasibly use this to their own end. The threats range from extraction of information about the targets blood sugar levels, stopping alerts being sent to the user or sending fake alerts causing the target to do harm to themselves.

This is a common theme for most embedded medical devices such as electronic pace makers and embedded defibrillators. Any sort of unauthorised access or interception of communications from the device could have lethal consequences for the individual fitted with the device.

As with both Industrial IoT and Consumer IoT devices the increase in adoption over the next decade will greatly increase the availability of these devices. This is a double edged sword. On one hand these devices have the potential to save many lives, on the other they are likely to have a lot more focused attention from bad actors. For some groups the prospect of being able to hold someone hostage remotely would be extremely valuable.

3. Ethical and Legal Considerations

Privacy and data security are two issues that can easily arise from poorly configured security surround IoT devices. IP Webcams are often deployed in offices of businesses to enable remote monitoring out of office hours and can cut down on the costs of an on site security team. Issues arise as IP cameras get cheaper and carry less security features such as a lack of encryption on the video feed. These cameras can pose a huge privacy issue when found on listings from Shodan with public facing login pages along with very often weak username and password combinations.

Lets take for example a camera that looks over a floor of office cubicles. The employees of this office will more than likely never really notice the camera as is the case with many out of sight out of mind IoT

devices. If this camera is actually streaming video openly to the internet there's a very high chance that an attacker could watch this stream and extract sensitive data such as passwords typed on a screen, record keystrokes if someones keyboard is visible or just record movements of employees in preparation for a physical attack. In this situation the business has both an ethical and legal obligation to ensure the security of their surveillance systems.

4. Security Concerns

4.1 Availability

When it comes to IoT devices a premium is often placed on availability followed by integrity and finally confidentiality (Harper et al., 2018). This is because when the service is no longer available it can cause huge issues, take the large Facebook outage in October of 2021 for example. While the initial outage was caused by a command accidentally making Facebook and related domains unreachable, the outage was prolonged by employees being unable to access the building to fix the issue (Heath, 2021). This was because the access card points were IoT devices that no longer functioned due to the outage. Taking this example we can theorise an attack vector on companies that utilise a similar method of building entry. Performing a denial of service attack via targeting the servers the door locks use to communicate or jamming the devices directly could render a business inoperable for a varying amount of time, depending on the degree to which IoT devices are relied upon in the running of the business.

4.2 Visibility

Any device connected to the internet is visible to anyone that looks in the right place. This process is made easy with the Shodan search engine. Using a variety of tags and filters we can see devices connected to the internet and the banners that they return.

Figure 3. A list of the most common HTTP titles returned by IoT devices in the UK.

Here we can see the top HTTP page titles of devices in the united kingdom being returned to us through Shodan. The top result is "401 Unauthorized" which indicates that the device has been set up correctly in order to stop unauthorised access. Interestingly the third most common result is "Vigor login page", Vigor is a brand of router made by DrayTek used across the UK and other countries.

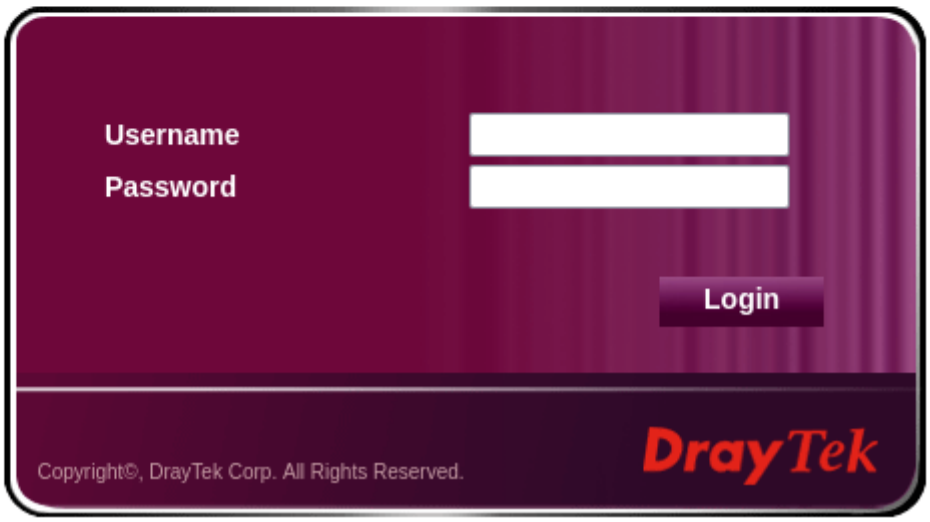

Figure 4. A login form served by a router exposed to the internet.

As these IP addresses are exposed to the internet we can easily connect and are then presented with a login page. While this doesn't inherently pose a risk to whoever's router this is, if they have failed to set up their device correctly an attacker can search for a list of default username and passwords, as seen below, to try and gain access to their network device.

Figure 5. A list of the default usernames and passwords used by various Vigor routers.

Access to the router in a network can allow an attacker to hijack DNS and steal users information with ease.

4.3 System resources

Due to the nature of IoT devices being small, low powered, low processing power systems. they often lack the resources necessary to run sufficient cryptographic algorithms and other security mechanisms. This can be seen clearly by finding IP cameras that are open to the internet. Most are using the RTSP (Real Time Streaming Protocol) protocol to stream their video remotely to a user wherever they want to access it.

5. Recommendations

5.1 Security Practices

5.1.1 Password Policy

Implementing proper password practices can severely limit an attackers options when trying to use an IoT device to gather information or as a toe hold on the network.

Figure 6. A graph of the most common usernames used in IoT attacks (Symantec, 2020).

Figure 7. A graph of the most common passwords used in IoT attacks (Symantec, 2020).

As can be seen from the above graphs, attackers are using easily guessable or default passwords when trying to access IoT devices. Failing to implement sufficient passwords on devices is akin to removing the password altogether and leaves your device open to anyone that can find it.

It can be argued that it is the manufacturers error in not implementing mandatory password changes during set up of devices, this is unlikely to change until laws surrounding the security of IoT devices catch up with the growth of the industry. In this intermediary time, the department responsible for setting up connected devices within the business should make sure that a secure password policy is baked into the security governance of the business.

This governance should layout factors such as:

Factor	Example
Minimum complexity	Capital letters, symbols, numbers
Time between password resets	3-6 Months
Password storage methods	Password manager, secured hard copies
Minimum password length	9 Characters

This could be implemented along side a thorough logging system for when new devices are added to the network to make sure none are left in a vulnerable state inadvertently.

5.1.2 Patching

Due to the shear number of connected devices likely to be utilised by a single enterprise, keeping up to date and implementing security patches could be extremely complex and time consuming. A remote connection to the device may not be possible to patch it so often the only option for patching some bespoke devices is to manually transfer the files to each device. An option to reduce the time and complexity of this task would be to limit the providers of devices you use. Keeping to one or two different providers will limit how many different sources of patches need to be monitored and reduces the risk of any single device being left in a vulnerable state due to negligence. If multiple vendors are used due to necessity, a concerted effort should be made to automate the monitoring of their respective RSS feeds and/or email lists to keep on top of the latest patches.

5.2 Device Security Standards

When considering what IoT devices to implement in the business it is highly recommended to find devices that adhere to standards such as ETSI EN 303 645 (European Telecommunications Standards Institute, 2020). Devices that follow these guidelines will be at far less risk of attack. While it may be difficult to find devices that adhere wholeheartedly to these guidelines it is recommended that IT and security departments familiarise themselves with the documentation and make their decisions based on that.

5.3 Network Traffic and Rules

If the business in question has an IT security department monitoring inbound and outbound traffic from IoT devices is an effective way of securing a businesses IoT solution. Monitoring internal network traffic will provide early signs of intrusion such as different IoT devices communicating with systems they wouldn't normally. Large IoT solutions can generate a huge amount of data so care should be taken to monitor key network choke points to keep data to a usable level. Using these tools allow and deny lists can be generated to prevent a single device leaving it's assigned scope.

Due to the limited processing capacity of IoT devices it will likely not be possible to deploy traditional host monitoring systems on each device.

6. Conclusion

As the IoT industry grows and becomes more integrated with the daily functions of consumers, industry and medicine, bad actors are going to shift their focus onto finding ways to exploit these new systems. In this period where manufacturers can legally ship these devices with limited or non-existent security features, the onus is unfortunately on the business investing in IoT solutions to make sure they choose the right balance between convenience and security.

Businesses adopting IoT solutions should ensure that any new device added to their network is surrounded by the appropriate security controls to monitor their behaviour. Logs of security patches should be kept and all relevant new patches should be installed at the earliest opportunity. Failure to ensure all devices are patched can easily leave a hole in the network for attackers to use as a toe hole to pivot towards the rest of the network.

Businesses that build up their security solutions surrounding IoT now will have an advantage as newer, more powerful IoT devices are developed that have more integrated security functions. Having sophisticated security policies and procedures will allow the business to reap the benefits of a full IoT solution while minimising their risks.

References

Brassfield, M. (2021). Smart devices more than doubled in US homes amid COVID pandemic. https://www.itpro.co.uk/mobile/mobile-phones/359826/smart-devices-more-than-doubled-in-us-homes-amid-covid-pandemic.

Diabetes UK. Continuous glucose monitoring (CGM). https://www.diabetes.org.uk/guide-to-diabetes/managing-your-diabetes/testing/continuous-glucose-monitoring-cgm.

European Telecommunications Standards Institute. 2020. Cyber Security for Consumer Internet of Things: Baseline Requirements.
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Ezell, S. (2016). IoT and Smart Manufacturing. https://www2.itif.org/2016-ezell-iot-smart-manufacturing.pdf?_ga=1.261819661.1089858538.1464487061.

Harper, A., Regalado, D., Linn, R., Sims, S., Spasojevic, B., & Martinez, L. et al. 2018. Gray hat hacking (5th ed.). McGraw-Hill Education.

Heath, A. 2021. Locked out and totally down: Facebook's scramble to fix a massive outage. https://www.theverge.com/2021/10/4/22709575/facebook-outage-instagram-whatsapp

Hossain, M., Fotouhi, M., & Hasan, R. 2015. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. 2015 IEEE World Congress On Services. https://doi.org/10.1109/services.2015.12

Lueth, K. (2020). State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. IoT Analytics. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

Patnaik, Ranjit & Padhy, Dr. Neelamadhab & Raju, Srujan. 2020. A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges. https://doi.org/10.1007/978-981-15-5400-1_68

Sinha, S. (2021). State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. IoT Analytics. Retrieved 25 November 2021, from https://iot-analytics.com/number-connected-iot-devices/.

Symantec. Threat Landscape Trends – Q2 2020. Symantec-enterprise-blogs.security.com. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-trends-q2-2020.

Trend Micro. N.D. Industrial Internet of Things (IIoT). https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

Westcott, K., Loucks, J., Littmann, D., Wilson, P., Srivastava, S., & Ciampa, D. (2019). Build it and they will embrace it. https://www2.deloitte.com/content/dam/insights/us/articles/6457_Mobile-trends-survey/DI_Build-it-and-they-will-embrace-it.pdf.