Research Report on a Cyber Security Topic

VU23217 & BSBINS401 - Cyber security in an organisation

STUDENT NAME: KELLY LINDSAY
STUDENT ID: 100694303

STUDENT NAME: REBECCA BROWN
STUDENT ID: 100692933

Research Topic Title: Hacking of Smart City Critical Infrastructure

Table of Contents

Introduction

Critical infrastructure is the essential services and systems which support the fundamental functions of a society and economy. These services are vital for the health, safety, and security of the general public, encompassing the energy sector, water systems, transportation, communications, healthcare, public safety, the financial sector, and more.

Smart cities are cities that use digital technology to manage resources and services, such as critical infrastructure, better. They use advanced technology to connect different systems like traffic controls, energy grids, and public services through the use of Internet of Things (IoT) devices to collect and share data, making urban life run smoothly and efficiently as a functional society and economy.

The amount and type of data and control that is utilised in running a smart city makes it critical to ensure that they are rigorously protected from cyber criminals, as the consequences of a successful attack can be devastating to not only the infrastructure of the city, but to the lives of everyone in the city. This report looks at how cyber criminals can target critical infrastructure in smart cities, the potential impact of such attacks, and how we can protect against these cyber threats.

Smart City Critical Infrastructure

The Internet of Things (IoT) and a vast array of sensor networks make up the backbone of a smart city. Key features of smart city infrastructure include smart traffic management systems, smart utilities, and public safety and surveillance systems.

IoT is crucial to building smart cities because of the connectivity it provides to the network of sensor technology that underpins their infrastructure, and enables real-time data collection and management. This network of sensors include:

- Electrical sensors (including but not limited to visual and audio sensors) to monitor things such as the environment, parking, speed, ect to improve the quality and security of city residents' lives,

- Chemical sensors to monitor environmental conditions to assist in managing health outcomes, and:
- Smart grid sensors to help manage the distribution of energy within the smart city.

Smart traffic management systems are a key component of smart cities, as they help to minimise congestion on the roads and improve safety within the city. IoT devices, such as radio frequency identification (RFID) and automatic identification and data collection (AIDC) tags, and interconnected CCTV cameras providing real-time monitoring of road conditions, along with connected traffic lights, all work together to better the flow of traffic, reduce response times to incidents, and overall enhance transportation systems within the city.

Smart utilities such as the electrical, water, and gas industries use feedback from consumers to ensure that the supply available is greater than demand, making sure that the connection to these services remain uninterrupted. Sensors help direct the flow of resources to where they are required so as not to waste resources where they are not needed, or undersupply areas. Sensors also identify faults in the system to facilitate maintenance and minimise infrastructure downtime.

Cyber Threats to Smart City Critical Infrastructure

Smart cities rely on a large network of interconnected devices to function. As the number of devices increases, so too do the opportunities for cyber criminals to exploit them. Physical and cyber security protocols (such as insufficient or poorly managed access controls, lack of staff awareness training, and inadequate response action plans) that are not robust, as well as the use of outdated software and hardware are common vulnerabilities that are targeted by attackers.. These breaches can have devastating effects on both the functionality of a smart city and the safety and well-being of those who live and work there.

Attacks that target traffic management systems can lead to the traffic control data being manipulated. This manipulation can increase congestion on the roads and severely impact response times of emergency services. Similarly, successful denial of service (DoS) attacks have the power to disrupt the supply of services, and prevent monitoring equipment from detecting faults and compromised systems.

Attacks on services or facilities that handle the massive amounts of data that smart cities rely upon to effectively operate can lead to sensitive data being stolen for ransom, sale, or used in other criminal operations. Data could also be manipulated, leaked, or deleted, facilitating the spread of misinformation, reducing public trust in both the security of a smart city's systems and the systems themselves, and can potentially compromise the safety of residents.

These potential outcomes highlight just how critical robust cyber security policies, procedures, and protocols are to maintaining the functionality of a smart city and ensuring the safety of its residents.

Case Studies

The Industroyer Attack on Ukrainian Electrical Substation (2016)

On December 17, 2016, Sandworm, a cyberwarfare group in the Russian military intelligence service, targeted a Ukrainian electrical substation at Pivnichna on the outskirts of Kyiv, cutting power to approximately 20% of the city. This attack was executed by a sophisticated malware package called Industroyer (also known as CrashOverride). The Industroyer attack was the first of its kind, in that it was designed using industry-level knowledge of the specific systems and equipment that is used in electrical substations, with the purpose of using these systems' own legitimate functions against itself.

While it's not entirely clear how Industroyer was deployed to the substation, an indictment issued by the United States District Court suggests that spear-phishing may have been involved. Once deployed, several payloads were activated on a countdown timer which opened all of the station's circuit breakers, causing the power outage. An hour later, a data wiper program disabled the computers at the station, forcing the staff to have to manually re-energise the system, while also hiding the malware from real-time detection.

A further module of Industroyer was designed to attack the Siemens SIPROTEC 4 protective relays using Denial of Service (DoS) to render them unresponsive. This would have been achieved by exploiting a bug in the device's firmware allowing packets to be sent to a specific port, a vulnerability that had been patched by Siemens in 2015 but had not been updated by the substation. This part of the attack failed as the commands were sent to the wrong IP address. Other modules in Industroyer include a "kill switch", designed to wipe all traces of the malware, and a trojanised working copy of Windows Notepad, which was intended to work as a secondary backdoor in case the main backdoor was detected or otherwise shut down.

The response to the attack was swift, with the Ukrainian authorities and energy sector staff restoring power within about an hour, and investigations commencing almost immediately on both a national and international level. Following the attack, new security technology was implemented at the Pivnichna substation, and better response plans and staff training were developed.

While the initial impact appeared lacklustre with power only being disrupted for an hour, particularly considering the complexity of Industroyer itself, it's in this complexity that the true threat lies. Cybersecurity experts at ESEC and Dragos theorise that this was not a one-off attack, but a "proof of concept" modular toolkit that can be relatively easily adapted to carry out more advanced attacks. It's also believed that had the DoS attack on the protective relays been successful, substantial physical damage could have been done to the electrical grid. The level of understanding of electrical systems shown in Industroyer highlights the time, resources, and intent that groups such as Sandworm are both willing and able to use to carry out potentially devastating cyber-attacks on critical infrastructure.

The Atlanta Ransomware Attack (2018)

In March 2018, Atlanta, Georgia (one of the largest cities in the USA) experienced mass disruptions to citywide operations due to a ransomware attack known as SamSam, which encrypted the city's data in exchange for payment in Bitcoin.

The attack impacted much of the city’s smart infrastructure, and caused mass outages to city services such as court systems and documents, police records, and payment systems for utilities and parking.

The attackers used brute-force techniques to access networks connected to Atlanta’s City Hall. The attackers used algorithmic password-cracking to secure credentials. Once they were able to access government networks, they then launched their SamSam ransomware into the system.

The attackers were able to first gain access through weak passwords, unpatched vulnerabilities, and compromised Remote Desktop Protocol (RDP). Once inside the network, they would escalate their access, before releasing the SamSam ransomware into the system. The SamSam ransomware used encryption algorithms to lock files and then demand payment.

Many of the city’s digital services were disrupted for several days. Key services such as online billing payments, court systems and public records were not able to be accessed. It is estimated the city incurred $17 million in recovery costs. While the attack did not result in any direct harm or loss of life, there was significant data loss and breaches to public records which greatly hindered police efforts on other cases. The attack also severely impacted the public’s trust, who questioned the city’s ability to protect sensitive information about its people. However, this attack caused an overhaul of the system, which then led to greater security and improved reputation and trust.

The city was quick to act and isolated systems to prevent the SamSam ransomware from spreading. Critical systems were taken offline, with cybersecurity experts immediately restricting access to the city’s networks.The recovery effort, however, took months. The city had to rebuild its system based on backups, which was made more challenging as the backup procedures were outdated.

The main lesson learned was that it is integral to keep systems updated, and that cybersecurity requires ongoing funding in order to maintain and ensure systems are able to anticipate new threats. Their entire cybersecurity policy was overhauled, with greater regulations on data protection and incident response, as well as cybersecurity audits. The incident was an eye opener for other cities, who also adopted better practices, including more regular data backups and multi-factor authentication to work against password-cracking algorithms.

Atlanta became a cornerstone for other cities to take note on the importance of cybersecurity, and prompted cities to establish more dedicated teams to cybersecurity. Atlanta illustrated how easy it was for attackers to take over, and the mass financial impact it can have as a result.

Consequences of Cyber Attacks on Smart Cities

As shown in the case studies above, cyberattacks can cause huge financial losses. Financial loss can be caused by demand for ransom from a ransomware attack or can be costs associated after the attack, such as loss of business operations.

In a cyberattack, essential services can come to a grinding halt. Services affected can include electronic payment systems, public and medical record systems, communication systems, and transportation. Operational disruptions can have devastating and ongoing effects, affecting not only businesses, but also the general public.

Reputation is important as the public and users may withdraw from sharing important personal information, which can impact the overall success and functionality of an application. It is paramount that a user can trust an application or they will not use it and technology will be deemed useless.

Preventative Measures and Cyber Security Strategies

As smart cities grow and the world becomes more heavily interconnected and reliant on technology, the ability to protect cyberspace becomes increasingly difficult. It has been essential within smart city architectures to introduce and implement best cybersecurity practices and protocol.

Governments worldwide have been integral in designing and establishing cybersecurity policy and frameworks to foster secure smart city infrastructures. In Australia, the Australian Cyber Security Centre (ACSC) plays a critical role in providing vital guidance to protect smart city infrastructure. The ACSC began operations in 2014 and has since become the Australian Government's technical authority on cyber security.

Services that the ACSC offers include:

- The Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- Publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- Cyber threat monitoring and intelligence sharing with partners, including through the Cyber Threat Intelligence Sharing (CTIS) platform
- Technical advice and assistance to help Australian entities respond to cyber security incidents
- National exercises and uplift activities to enhance the cyber security resilience of Australian entities
- Collaborating with Australian organisations and individuals on cyber security issues through ASD's Cyber Security Partnership Program.

Government initiatives are crucial in developing a secure smart city infrastructure. Governments are important as they;

- Establish national security standards
- Fund research
- Foster collaboration between public and private organisations
- Encourage international collaboration
- Create and enforce law
- Provide education and awareness

It is important for public and private organisations to forge strong partnerships by sharing information regarding cyber security, in order to build resilience against existing and future cyber security attacks. Some initiatives to foster shared information include;

- The Cyber Threat Intelligence Sharing (CTIS) – a threat information sharing platform.
- Digital Identity and the Trusted Digital Identity Framework (TDIF) – a foundation for establishing secure, trusted digital identities.
- Security of Critical Infrastructure (SOCI) Act – provides the government with significant powers to respond to cyber-attacks on critical infrastructure.

Another preventative measure in cybersecurity is continuous monitoring and incident response planning. Having an effective incident response plan means that there is a structured approach to contain and mitigate against threats. In combination with continuous monitoring, organisations can act quickly to defend against any malicious software attacks.

Future Trends and Challenges

As technology continues to evolve, cyber threats are ever imminent. Emerging technologies such as AI and 5G are popular, but offer new channels for cyber criminals to attack. While 5G may offer speed and better connectivity, it offers an expanded attack surface and potentially more vectors or attack points for cyber attackers to use. It is therefore essential that cyber security is able to adapt and evolve in order to combat potential threats within smart city infrastructures.

Smart city technologies are evolving at a rapid pace. The world has an insatiable need for the newest technology, meaning that cybersecurity needs to continually evolve to keep in line with this technology. Organisations need to have scalable, multifaceted and adaptive security protocols in place in order to have the greatest protection against changing cyber threats.

Another challenge to cybersecurity is international collaboration. The world must share knowledge and adopt best practices to combat threats effectively. However, international agreements and partnerships can be strained as each individual country seeks to protect its own classified information.

Looking beyond 2024, smart cities will require continuous evolution in the cybersecurity space. A strong commitment to international cooperation, public-private partnerships and adaptive policy frameworks will be required for the success of smart city infrastructure.

Conclusion

In conclusion, a smart city is a complex ecosystem that requires multifaceted security planning in order to protect its critical infrastructure from malicious cyberattacks. Without security frameworks, the effects of cyberattacks can be devastating, leading to mass operational disruptions and financial losses. By fostering partnerships between public and private organisations, as well as continually sharing information on cyberattacks, smart cities can work together to protect their critical infrastructure and create a safer cyber community for all.

References

Alharbi, N. & Soh, B. (2019). Roles and Challenges of Network Sensors in Smart Cities. *IOP Conference Series: Earth and Environmental Science, 322*(1), 012002. https://doi.org/10.1088/1755-1315/322/1/012002

Australian Signals Directorate. (2020, Oct 14). *Who we are.* Australian Cyber Security Centre. https://www.cyber.gov.au/about-us/about-asd-acsc/who-we-are

Batka, V. (2022, November 7). *Why a 'Living security' approach is needed for smart cities to thrive - Australian Cyber Security Magazine*. Australian Cyber Security Magazine. https://australiancybersecuritymagazine.com.au/why-a-living-security-approach-is-needed-for-smart-cities-to-thrive/

Deloitte. (2022, May 27). *The Importance of Public-Private Partnerships in Australian Cyber Resilience.* Perspective. https://www.deloitte.com/au/en/services/risk-advisory/blogs/importance-public-private-partnerships-australian-cyber-resilience.html

Gilbert, D. (2017, January 15). *Ukraine's power station hack is a stark warning to the rest of the world.* Vice.com. https://www.vice.com/en/article/ukraines-power-station-hack-is-a-stark-warning-to-the-rest-of-the-world/

Haiston, J. (2024, March 11). *What is a Smart Traffic Management System*. Symmetry Electronics. https://www.symmetryelectronics.com/blog/what-is-a-smart-traffic-management-system/

Institute for Defense & Business (2021, July 19). *What Are the Cybersecurity Risks for Smart Cities?* https://www.idb.org/what-are-the-cybersecurity-risks-for-smart-cities/

Miller, C. (2021, August 19). *Throwback Attack: SamSam hobbles the city of Atlanta with an extensive ransomware attack.* https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-samsam-hobbles-the-city-of-atlanta-with-an-extensive-ransomware-attack/

MITRE ATT&CK ®. (2024, April 11). *Industroyer, Software S0604.* MITRE ATT&CK ®. https://attack.mitre.org/software/S0604/

Shea, S., & Burns, E. (2020, July 16). *What is a Smart City? Definition from WhatIs.com*. IoT Agenda. https://www.techtarget.com/iotagenda/definition/smart-city

Smart City Cyber Security. (2023, June 6). *Smart City Threat Scenarios.* https://smartcitysecurity.net/smart-city-threat-scenarios/

Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. (2021, March 30). IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities, 4*(2), 429-475. https://doi.org/10.3390/smartcities4020024

Slowik, J. (2019, August 15). *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.* Dragos. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

U.S. Department of Justice. (2020, October 15). Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace [Press release]. https://www.justice.gov/opa/press-release/file/1328521/download

Young, K. (2021, Sept 20). *Cyber Case Study: City of Atlanta Ransomware.* Case study, Cyber Liberty Insurance.
https://coverlink.com/case-study/city-of-atlanta-ransomware/