Cybersecurity Critical Infrastructure Effectiveness on Cyber attacks

Jaden Howell

Cybersecurity undergraduate at Old Dominion University

For Professor Michelle D. Heart

English 231C

Abstract

In cybersecurity, a main point of concentration is always the critical infrastructure. In the traditional world, the critical infrastructure would be a compilation of many different things that keep society together. However, in the cybersecurity sense, the critical infrastructure is more precise and valuable. With that in mind it means that more steps need to be accounted for in terms of protecting it against threats and attacks. Within the research project I carried numerous test on the critical infrastructure to determine vulnerability and awareness as well as setting up an algorithm that can better assess situations that appear almost instantly within the critical infrastructure.

Introduction

Critical infrastructure is the basis of all of the technological advancements in this day and age. In a way it is the spine that holds everything together and keeps it stable. Without the critical infrastructure, technology would not be how it is today. There is a physical and technological aspect about it that needs to be protected against harm. The physical part of it would be the computers and the physical data centers that you may see within a building. They may not look like much but those pieces within the buildings hold a lot of the data that people store. It is very important that the physical components stay safe in order for the privacy and protection of the people is insured. For the technological and nonphysical aspect of the critical infrastructure, it is made up of more parts. One major one would be any firewall within the system. The firewall is basically apart of the security aspect of it that monitors the activity going on in the network and filters traffic that is either needed or not needed. Because of that, it is essentially one of the first lines of defense that would allow the company or major system to know when there is a threat or risk at hand. These two different parts of the critical infrastructure make up its entirety and, on both levels, they need to be protected and made sure that they can carry out their purpose with no issues.

Obviously, the main source of damage to the critical infrastructure would be cyber-attacks. Cyberattacks have a variety of different forms and it can be challenging to figure out when, where, and how they happened. The interesting thing with cyberattacks is that it does not have to be a major company or military force who does it. Anyone with the knowledge of the technology could very well try to attack could do it if they knew what they were doing. Normally when you hear about hackers, it is only a select few committing the attack. With that in mind, it is uncertain when the next one could be and how massive the attack will be which is why it is important for the critical infrastructure needs to be protected. If the critical infrastructure goes

down, then that could be a huge loss for the company or business or whoever is affected by it. It could also lead to a major freeze in technology and could stop the advancement of technology if the attack was on a more grand scale.

The key factor with protecting against cyber attacks was to establish a better system overall with how to deal with threats and what to do in certain situations as well as the best approach. Starting off with figuring out the best course of action against cyber attacks can prove effective in the long run with negating them while they happen or even before they can do any real damage. Halima Kure stated that “Proper operation of the assets is essential for such a system and any threats that could negatively impact the asset could have a severe disruption” and that “Risk management is an important aspect of the protection of CI”. Without understanding the risk and how to maintain and secure vulnerabilities, the critical infrastructure is at a high risk of being sabotaged. Risk management can only go so far however, which is why there needs to be a more technical risk management that needs to be able to assess and dilute a situation before major chaos happens. Whenever a threat is identified, more likely than not it is already too late, and the system is compromised.

Methodology

The study involved two phases. The first phase was that the main group of researchers and people in the field were hands on with making sure the system was about to detect and defend threats effortlessly without any glitches or faults. The second phase was to create a system that could algorithmically detect and defend threats without needing assistance. Initially the project was going to be mainly focused on phase 1 due to the fact that there were ample

enough of workers that could be able to defend the system. However, after a bit of experimentation we figured out a way to create a system that could be completely hands off and self-sufficient which would relieve people of the stress of locating and figuring out attacks. This system would be productive all across the globe for whoever decides to use it and it allows for the people around the system to take measures in other specific areas where they see fit.

Phase 1 was in motion by setting up different scenarios of attacks. Penetration testers and ethical hackers were in charge of essentially finding out about the vulnerabilities in the critical infrastructure and, if possible, see if they could find alternative vulnerabilities for the same part of the infrastructure. What that means is that if they were to find a exploit in the system, they would analyze it and see if there was another way that the exploit can be accessed. The reason why we started with this is so we could strengthen the core of the critical infrastructure to make it almost impossible to penetrate through. Once that was established, the other main focus was with detection throughout the system. Whether it was through intentional means or through a possible breach, it was imperative that the critical infrastructure could alert authorized individuals of activities going on throughout it.

Phase 2 was simply just using all that was collected in phase 1, but implementing it into a algorithm that could do the same work that would require people to do. Instead of having people go in and try to secure the threat, the algorithm would be first in regard to threats and attacks. It would be adaptive within milliseconds and would show reports to the authorized individuals of what has happened in the critical infrastructure. The algorithm would be processed to know all of the components within the critical infrastructure and would know exactly how to defend against any and every attack or threat. Essentially it would be a supercomputer capable of doing exactly

what a group of people would be doing. The people working there would be backup if there is truly a case where the algorithm fails.

Results and conclusion

The results were exactly what was projected at the start of the project. Both phases carried out what they were intended to do and now the algorithm has been created to ensure the protection of the critical infrastructure. After running the algorithm in various forms of penetration tests, the results came back that it perfectly neutralized the threat and made reports about the incidents as well as informed us as soon as the incidents started. During phase 2, we had intended to only incorporate phase 1 as the main phase if it turned out that the algorithm was unable to perform however the algorithm successfully did the tasks embedded inside of it. It now can work at full capacity without need of supervision or configuring. It does the peoples job more efficiently and allows for the critical infrastructure to stay secure and monitored at all points of the day and night. The project finished earlier than the projected time that was estimated which meant that the research findings and reports could be published earlier for the sake of society and the future of technology.

Discussion

The major reason as to why this study was carried out was so that the future of technology would never have to be in a state of fear of being set back. Although the general population would not understand the breakthrough of this project, the people within the

technology division would be amazed at what was accomplished in the time this all took place. This study was to both improve the critical infrastructure and to decrease the probability of cyber attacks being sent out to major entities. Not only could cyber attacks be done within the same society, but they could be done across nations which could create cyber warfare. It may not be as lethal as a traditional war, but a cyber war could still impact a nation in numerous ways. With this study and technology, this ensures that whoever has the ability to create this algorithm will be more protected than before. A major factor with this project is whether or not companies or even nations have access to the technology and information needed to go into this plan which means that there will be a technology race to ensure that they have it. Because of this study, it will open doors to more types of research projects centered around the critical infrastructure and technology. Technology is a growing field and will always grow and expand so it is important that it is always advancing for the greater good.

References

https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-cps.2018.5079

Kure, H., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems, 4(4), 332-340.

https://www.proquest.com/docview/2315522700?pq-origsite=primo&accountid=12967

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. Applied Sciences, 8(6), 898.

Alshboul, Y., Bsoul, A., AL Zamil, M., & Samarah, S. (2021). Cybersecurity of Smart Home Systems: Sensor Identity Protection. Journal of Network and Systems Management, 29(3), Journal of network and systems management, 2021, Vol.29 (3).

https://www.proquest.com/docview/2495794054?pq-origsite=primo&accountid=12967

Leevy, J., Hancock, J., Zuech, R., & Khoshgoftaar, T. (2021). Detecting cybersecurity attacks across different network features and learners. Journal of Big Data, 8(1), 1-29.

https://www.proquest.com/docview/2492469202?pq-origsite=primo&accountid=12967