Cybersecurity Breach

Berline Najacque

School of Cybersecurity, Old Dominion University

CYSE300: Introduction to Cybersecurity

Professor: Malik A. Gladden

September 10, 2023

Cybersecurity Breach

Since the infancy of the network via the Internet, hackers have been striving to breach networks in order to steal companies' secret documents, sensitive government information and the likes. Cybersecurity has been created to prevents those kinds of illicit actions. These hackers could be one person that could work by himself using blackmailing to get some quick money or it could be a group of computer experts, who work for the government in order to spy and get industrial information, federal government sensitive data. I want to elaborate the breach that had happened in a water treatment plant in Oldsmar, Florida in February 2021. In this essay.

I am going to emphasize on the Vulnerability of cybersecurity, threat that could be exploited, the repercussions of a breach and measures that could be established to curb such attacks. When you are working for a computer company as an administrator, or as cybersecurity officers, one thing should come in mind: What is good for the system or the company? In this case, the hacker had used TeamViewer to get access to the water treatment network. TeamViewer is a remote access software that allows people to connect to another computer from anywhere in the world. In most cases users install TeamViewer on the desktop computer.
It is always good to use strong password and change these passwords every two weeks to prevent attack from hackers. One should use the latest operating system to make sure everything is running smoothly.

According to (New York Time) the significant component of drain cleaning, sodium hydroxide, was modified by the hacker from 100 parts per million to 11,100 parts per million. These are unsafe amounts that, if they had reached homeowners' houses, might have seriously.

poisoned them. This breach of security could have been a devastation for the community and the health department.

There are many ways a cybersecurity officer could mitigate these attacks. First is to train their technicians different ways how the network could be breached, what to expect and what to do in this situation. Second, do not use TeamViewer in the system, ensure that every piece of sensitive data is encrypted. On the other side, data encryption restricts access to data to those who possess the encryption key. Third is to use strong password so to make it difficult for criminal to access your data.

Additionally, one should make sure that even if unauthorized individuals access the data, they are unable to read it. Some data encryption tools even alert you when someone tries to change any information in the system. Fourth, use the latest version of operation system to make the operating system runs smoothly. Fifth, increase the cybersecurity force. Keep the system updated to prevent, hackers with bad intentions, who can write code and use to take advantage of security holes. This code is usually sent to you in the form of malware, which can damage the whole system. To keep one's information safe, make sure you use a patch management system that handles all changes automatically. In additional pay attention to physical security and install firewall to protect you from brute attacks or prevent security incidents from causing irreversible damages.

In our society as always, thieves had existed and will always exist. As part of the society especially nowadays where ninety percent of us have access to the internet and since we are doing so, we should always be aware that our computer, cell phones, iPad and the likes cand be hacked at any moments. In our technological society where almost all our transactions are being done by computers whether it is to get your driver's license, your license plates, birth certificates,

marriage license, death certificate, banking, buying using credit or debit cards etc.… Remember that none of these actions would be possible if the internet did not exist. Since this is so, one should be aware and be careful not to get into sites that hackers use as traps to get access to your personal data. Hackers also use phishing to get you to reveal your password and your banking information. Personally, the worst that could happen to a person is to get his/her identity stolen. There are some companies that are being scrutinized every day by hackers trying to get industrial information. We know the threats are there, therefore it is up to us be prepared and take countermeasures for all computer viruses, malwares in building effective firewalls, conduct testing in your network, have trainings for your cyber technicians and use the latest operating system so that the program could run smoothly and effectively.

References

10 ways to reduce cybersecurity risk for your organization: Upguard. RSS. (n.d.-a). https://www.upguard.com/blog/reduce-cybersecurity-risk

The Oldsmar Security Breach: What your utility needs to know. West Monroe. (n.d.). https://www.westmonroe.com/perspectives/in-brief/oldsmar-security-breach-what-your-utility- needs-to-know

Robles, F., & Perlroth, N. (2021, February 9). *"Dangerous stuff": Hackers tried to poison water supply of Florida town*. The New York Times. https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html