Matthew Fink

Cyber War AAR

Prof. Sabal

12/16/21

On the Defence

During the second to last week of the fall of 2021, Cairn University's Cyber War was underway. The cyber war consists of the Red Team and the Blue team, which we have discussed thoroughly throughout class; including but not limited to the tactics of both the attackers and the defenders. Different ways to monitor traffic on the network and many different ways to find vulnerabilities within the network. The goal of this project was for the blue team(the defenders) to protect a certain phrase that was made up by the professor, that phrase being “CAIRN University CIS421 CyberWar Blue Team Prize 2021”. This was the phrase that would win them the war, and they needed to protect it by using the methods that were shown in class. A couple of them being encryption and honeypots. The defenders could pick a spot anywhere within the network to hide the phrases and/or honeypots wherever they pleased, and try to spoof the attackers to buy some more time before the end of the week. The attackers objective of this project what's to find that phrase, and change it from “ Blue Team” to “ Red team” they would then have to re-encrypt their own phrase and then find a spot within the network just like the blue team did. And then the roles would reverse. The Blue Team would then be attacking with the red team defending. This exercise would last exactly a week starting from 7 a.m. on Monday on the 6th of December.

During this exercise I was a member of The Blue Team. Our objective was to hide that phrase. The very first thing that we did was set up a meeting to come together and talk about what kind of encryption methods we could use where we could actually hide the phrase what Honeypot we were going to use and how we were going to monitor the network. I was given the responsibility of finding the encryption method that we were going to use for this project and was our first task in beginning this project. We use a type of encryption called the vigenere Cipher, Which is basically just a fancy phrase for shift. And what we did was we had a key phrase which was the word “Macys” as well as the phrase we were trying to hide, and we basically did a shift of letters adding the value of the first letter of the key word, as well as the first letter of the phrase, combining the numbers that are associated to that of the alphabet and subtracting that number by one. Then that number would be associated with the letter in the alphabet and is what would be used to replace the letters in the phrase. The key word was actually convenient because we were able to split the phrase into three separate parts which we all then split the duty of encrypting the phrase together. The next objective was to place the encrypted phrase somewhere within the Cairn University Network. We were given a tip by Professor Sabal that a good place to hide it would be in the storm data database; this was a previous database that we used in an earlier course of our college career. We then as a team agreed to hide it within that database as there were thousands of entries already entered into the database and would have been easily hidden among all of them. Kali and I sent our encrypted portion of the phrase to Ken who then entered the encrypted phrase Into the Storm data database. We then decided to have Kali set up a few honey pots within the storm data database, and on to another student's account which we had previously had access to. These honey pots worth row off any traffic that the attackers may have seen throughout the week. These honey pots consisted of a very similar phrase but had very slight differences, and the goal of the game what's to have the exact phrase word for word. Ken then thought of a great idea to set up a program that automatically checks the database at midnight and completely replaces the phrase with its encrypted self. so this way if the attackers just so happens to leave the phrase where it was to throw us off it would have been immediately reversed because of our program. It was also set up to notify us if the data were to have ever gone missing or been changed.The week was pretty quiet in terms of traffic within the network but we had heard some talk that the other team was working extremely hard to find our phrase. Unfortunately for them they were not able to change the phrase to “Red Team” which crowned our team the victors. But after this Victory I spoke with members of the other team and learned that they spent many hours a night trying to understand what we had done to our phrase. and something that interested me was that they were able to find where we had hid our phrase. but the most difficult part for them was being able to decipher it. Dan, who is part of the other team, showed me a list of things that they tried to do in Microsoft Excel; such as different decryption methods, methods of attacks, and what they were going to do once they were able to decipher it. To the best of my knowledge they were on the right track and I was notified that they had the correct pattern but they were unable to figure out what the key word was. and to my estimation if they would have had an extra day or two they would have been able to crack our encryption and change the phrase. Luckily for us, they ran out of time and we were able to win the game.

The biggest thing to me that stuck out the most was how quickly they are able to move and open my eyes 2 the real world where hackers have unlimited time to figure out the encryption of something. there are less rules for them than there were for us. For instance they have the advantage of being able to do things that are illegal, but that was something that we could not Implement into our game. A report by IBM stated that there was an estimated 4.24 million dollars for the average cost of a data breach. Obviously this is no small number and can easily put a young business out of commission. During the pandemic of 2020Businesses were forced to quickly adapt their technology, with many IT companies encouraging that all employees work from home, most of which also moved into Cloud based activities. IBM stated that security within all companies may have been lagging behind due to these rapid IT changes. Which then left most of the country vulnerable to hackers with experience.(IBM) Many people of all companies around the United States easily had their credentials compromised which then led to the compromisation of data within their company. This apparently was a common occurrence with 44% of those credential breaches being the root cause.(Notified) one thing that actually surprised me was that the option of AI within many of those companies actually was one of the top three mitigating factors in reducing the cost of a breach, saving many companies an average of $1.25 million and $1.49 million. “Companies studied that adopting a zero trust security approach are better positioned to deal with data breaches. This approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources. Organizations with a mature zero trust strategy had an average data breach cost of $3.28 million – which was $1.76 million lower than those who had not deployed this approach at all.”(IBM) This however is one of the more involved strategies when trying to keep your data safe. companies had to break their backs by going through every single one of their employees and either changing all of their credentials or just changing their passwords. and with a company with a few thousand workers could be a huge problem as there could be many different entry points that a hacker could have attacked from. The legal ramifications of these data breaches can be extremely harsh on a company especially if customer data has been exposed publicly.

California, New York and Nevada have led the field in state-level consumer privacy, with Nevada’s Consumer Privacy Law due to be enacted on October 1, 2019, and California’s CCPA and New York’s Privacy Act coming into effect on January 1, 2020. Covered businesses are required to be up front and transparent in the event of a cyber-attack, and must demonstrate a commitment to resolve the issue lawfully. Observing the law this way can help to reclaim a positive standing and mitigate further damage. In the event of a data breach, there are four legal implications enshrined in data protection laws across all jurisdictions. They are Notification, Response, Penalties, and Litigation. The first three are fairly straightforward, but the litigation is where it can get complicated. In some cases a company might be subjected to private lawsuits brought by customers and shareholders because of the result of a Cyber attack and with that comes the anticipation of legal issues. Such legal issues could be fines, penalties, or even jail time for the party that was involved in the data breach. Legally all companies have an obligation to protect the information of their customers.(Taylor) But the easiest way to prevent any attack on your company is to always be prepared. You never want to lag behind in this ever-increasing technology world that we are living in. Something that was said in class was that you don't want to be the low-hanging fruit and that nobody is ever truly protected from an attack; it's all about not being the first to get found.

Citations

IBM. (2021, July 28). *IBM report: Cost of a data breach hits record high during pandemic*. IBM Newsroom. Retrieved from https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

Notified. (2020, January). *2020-data-breach-report*. Itrcnotified. Retrieved from https://notified.idtheftcenter.org/s/2020-data-breach-report

Taylor, B. (2021, July 30). *Data breach: The legal implications*. The Data Privacy Group. Retrieved from https://thedataprivacygroup.com/blog/2019-9-17-data-breach-the-legal-implications/