Short Research paper #2

Nicholas Robertson

CYSE 300

Dr. Joseph Kovacic

January 25, 2023

Information is the most important asset within any company, and it is the life blood that makes and breaks any business. To keep that information safe and secure requires a strict set of rules that must followed by every employee. Threats to the system can be comprised of a variety of different attacks that not only effects software and hardware, but also human factors as well. Security issues like phishing attacks, viruses, worms, password protection, and espionage. These threats to the system can be disastrous if they're not taken care of and needs to be addressed and identified so that threats can be avoided before they become an all-out breach.

Social engineering is one that doesn't have anything to do with hacking or using direct attacks to steal information. Instead, it's hinges on the idea that the attackers must use social tactics (i.e., tricking someone though mental gymnastics) to accomplish their goals. This is commonly found in phishing and whaling attacks, which are attacks designed to look like legitimate emails from a company manager but are meant to steal the users' credentials. Phishing emails are targeted towards the employee's end, and it will usually say something along the lines of, "your password is out of date, click here to reset your password.". The link will open and steal your information, like username and passwords to gain access to the system under your name. The more targeted version of that would be spear phishing, in which the email will usually call out the induvial in name, or mention something else personal about them to have them to make is seem even more legitimate, so that you will click on the link. Finally, you have whaling which is where a manager or CEO is hit by a phishing email. The best course of action when it comes to these attacks is to take the time and look at who sent the email and if you don' know for sure never click on it. Ask your IT department to make sure that the email sent to you is real or not.

I've decided to combine both worms and viruses together to are in many ways similar to each other, with the only really big difference between them being, "how they self-replicate, with viruses requiring the help of a host and worms acting independently." (Nica Latto, 2020). For viruses these attacks can consist of ransomware, spyware, trojans, keyloggers, etc. Ransomware will hold your files and information hostage until a set amount of money is paid out. Spyware will spy on your system undetected to steal information. Trojans will disguise themselves as legitimate software and then plant a malicious virus onto your computer to either steal or destroy your computer. Keyloggers will pinpoint out the keystrokes on your computer to figure out login information, to then use your logins to infiltrate the system at work. Worms on the system, can const of email worms, file sharing worms, etc. These two types of worms are very similar in what they do, the only difference, being is that one is attached and distributed (unknowingly) though email, while the other one is though files and they both rapidly spread without any input from a human. Avoiding these isn't hard, in fact the best thing to do is for companies to block employees from accessing and downloading suspicious files from unauthorized sites. But one of the most crucial things that can be done is to update the company's security systems; installing anti-virus software and firewalls the best cost-effective ways to crack down on this.

Human error is an issue that originates inside the company rather than an outside of the company. To give you an example of human error that a lot of company's face, lets take password protection for instance. According to a survey done by the website security magazine, out of the 2,000 people they surveyed "44 percent of respondents admitted to using their personal password at work." (Security magazine, 2020). Passwords are something that should be taken seriously on a daily basis, employees need to make their passwords they log into the system with complex and different from any other password that they might log into a different website with.

On top of that do not store your password in a compromising place. Don't just write your password down a sticky note, then stick it to the side of your cubical for a quick reminder and do not store it on your work or home computer. Instead write it done on a piece of paper and lock it within a lock box or file cabinet within your workspace for safe keeping. Also make sure you change it every few months. Human error has a lot more contributing factors like, forgetfulness and speed working, but these can be managed by simple solutions like monthly training videos and company meetings that refresh the employee's memory.

Espionage and bad actors within the company can sometimes be unavoidable. You hire someone for the company because you think their good fit, only for them to have alternative motives and then try and steal for within the company. You can never really tell who it could be, but you can avid it for the most part. Simply put, you need access control within the company to prevent people from gaining access to file within the database, who have no reason to be in there. For instance, a CFO of the company will need access to the financial records within the company, to do their jobs. To access that information, they will need special credentials and privileges within the company that no one else is allowed to have. If a ground floor employee logs into one of the computers at work, they should only see what they are allowed to see, they should not be able to see the same thing as the CFO. This keeps sensitive information from getting out into the public and to other companies. Make sure that former employee's credentials are wiped from the system, so they have no way of getting back into it after their gone. Finally implement hashing to keep notes on files that have been modified. Hashing allows companies t to see who last had access to what specific records and what was changed in said records on what date. This will prevent false information from permeating throughout the system.

There are many more threats that can infiltrate an information system within a company. While these are just a few, they are not to be taken lightly. Protecting customer information and companies' information is the best way to stay ahead of the competition and stay in the good graces of the public. Taking this seriously can also keep your company out of legal and financial troubles to. Remember information is the life blood of any company and your company will collapse without it.

Work Cited:

Nica Latto (2020), Worm Vs. Virus: What's the difference and Does it Matter? *Avast Academy* https://www.avast.com/c-worm-vs-virus#:~:text=In%20brief%3A%20Viruses%20and%20worms,spread%20without%20any%20human%20activation.

53% of People Admit They Reuse the Same Password for Multiple Accounts (2020) *Security magazine* https://www.securitymagazine.com/articles/92331-of-people-admit-they-reuse-the-same-password-for-multiple-accounts