DATA LOSS PREVENTION

LEE ACHEAMPONG

CYSE 250

12/7/2022

ABSTRACT

When it comes to cybersecurity, the protection of data and access is the most important task that there is. Preventing Data loss requires many factors of security and education. With the rapid and constant evolution of technology, security measures must also be up to par with these changes. These days, companies are responsible for protecting massive amounts of user information and access, and it falls on them to ensure that this sensitive information does not fall into the wrong hands. This is because not only could the leak or breach of personal data be highly harmful to users' privacy, but it can also invite hefty lawsuits against companies. So it truly is in companies' best interest to have well-functioning data protection and plans in place in case breaches or leaks do occur.

KEYWORDS: Data Loss, Data Loss Prevention, Security, Data

INTRODUCTION

With record-high levels of information and data being transferred at high speed, finding a proper and effective way to protect data should be at the forefront of securing private data. Data Loss Prevention is the strategy of preventing unauthorized access to sensitive data using a myriad of techniques and tools to deter attacks and attackers. It is extremely important for companies to have data loss prevention practices in place, as well as have these practices updated whenever necessary due to the ever-growing and changing forms of attacks. These attacks can have a lasting impact on a company's credibility, customer satisfaction, and retention, as well as have an impact on legal issues. Ensuring that data is kept safe and secured at all times, there are many different approaches to consider in order to protect and secure data from being accessed by unauthorized individuals. Data loss can occur in a variety of ways. While attacks such as ransomware or malware are the most known causes, there are also factors like employee sabotage and incompetence that can also lead to data loss. Malware attacks are when malicious software attacks a computer system by gaining access and executing unauthorized actions not usually known or instructed by the system's owner. A ransomware attack is a type of attack that threatens to publish or restrict access to a computer system or data until the victim of said attack

pays a ransom fee to the attacker. Both these types of attacks can devastate companies and leave them vulnerable to even more threats.

DATA LOSS EVENTS

One of the most impactful ransomware attacks to occur in the last couple of years was definitely the Colonial Pipeline. This ransomware attack occurred on May 6, 2021. The Colonial Pipeline is one of the largest oil pipelines in the United States as it provides oil from Texas all the way to New Jersey. With the number of states dependent on this pipeline for oil, it is extremely necessary to have proper protection and security in place so as to not have attacks that could potentially cripple half the nation. It was identified that the group of hackers that were responsible for this ransomware was known as DarkSide.

During the attack, a group of hackers, DarkSide gained access to the Colonial Pipeline and infected the pipeline's computer system, forcing the operations at the Pipeline to be shut down for several days. This ultimately led to a price increase in gas, and more frequent gas shortages on the East Coast. The group of hackers initially gained access to the Colonial Pipeline system through an exposed VPN password, which they then prompted to steal 100 gigabytes of data to use to hold a ransom over the Pipeline, threatening to leak the data on the internet if not paid. It was later discovered by investigators that the password that granted the hackers access to the system belonged to a Colonial Pipeline employee but was leaked when the employee used the same password in a different place. The attackers demanded a ransom of 4.4 million dollars, which Colonial Pipeline obliged, and thus were able to resume operations on May 12, 2021. The following month after the ransomware attack, the Department of Justice tried to recover the money lost, and to their efforts, they were able to gain 2.3 million out of the 4.4 million paid. An event of this magnitude could've had even more dangerous and lasting impacts had it continued and not been resolved, as quickly as it had been.

The Facebook scandal that occurred with Cambridge Analytica is another example of data loss. Prior to the 2016 election, Cambridge Analytica, a company based in the United Kingdom was able to access information from Facebook. Cambridge Analytica began accessing this information by creating a quiz on Facebook. This quiz was meant to collect information about all quiz takers, but unbeknownst to the quiz takers, the quiz was not only siphoning data

from the quiz takers without their knowledge but also users that the quiz takers had interacted with on the site, or had friended on the site. This information was then used to classify and target people. There was perfectly curated information that was targeted at different people to make them more susceptible to certain things. This perfectly curated information would be used to sway people's minds and ideas on certain topics. Cambridge Analytica later shared this data with the Trump Administration, which was then used to target voters and sway them to vote for Trump. This gross misuse of data by Cambridge Analytica definitely shows that Data Loss Prevention is very much needed. Having Data Loss Prevention policies in place can drastically lower and even prevent gross misuse of user data and even company data.

Another factor that is likely to cause data loss is victim precipitation. Victim precipitation theory is the theory that suggests that the actions of a victim can cause the crime. This usually pertains to when a victim will put themselves at risk, usually due to incompetence and then attackers taking advantage of them. An example of this is when some companies would actively broadcast that they have an ironclad security system that no hacker will be able to penetrate their systems. In this instance, the company or organization calls attention to themselves and in doing so creates a target for malicious attackers to attack and penetrate their systems, causing them to lose data as well as weaken their defenses for their systems. This can also cause companies to lose access to their system, as an attacker might demand a ransom, usually monetary until the company pays them. Although it isn't the most common method that usually leads to data loss, it is still important to acknowledge that these types of instances do happen, and it is best to find solutions around them and prevent the loss of information and data.

Data loss can affect virtually anyone, but there are groups of people that are more prone to having their data lost, and systems accessed by unauthorized users. These people are usually digital immigrants. Digital immigrants refer to individuals who were born and raised in a time period where there was no use of widespread digital technology. These individuals are usually older people who were born and lived a great chunk of their lives without technology as it is today. These individuals still do own businesses that utilize technology and thus must be secured. The lack of digital knowledge for some of these individuals can truly be their downfall if their business or company is attacked digitally. Suppose a mom-and-pop shop uses a website and uses

their website to perform functions such as reservations, and advertising. A malware attack that shuts down their site, as well as steals data from their customers can heavily impact productivity. With customers that are well accustomed to the restaurant's site, this inability to use the site might sway them to other places, making the owners lose money. The owners of the restaurant might also lose their credibility. These factors can have lasting impacts on a company or business, especially one as small as a local mom-and-pop restaurant, which they could potentially never recover from fully.

PREVENTING LOSS OF DATA

Data loss can seem daunting and extremely unexpected in most cases, so it is critical the proper security infrastructure and policies in place to deal with them as they arise. When discussing solutions to combat data loss, there isn't just a one-and-done thing to do to ensure that your data is protected but rather a plethora of methods to utilize, depending on how big your organization or business is, how much data you own or operate with, and what security systems you already have in place. Other factors can also include who else also has access to your data, usually other staff members, and also the level of access that they have. All these factors must be accounted for when ensuring the security of your data because you do not want a minuscule detail to be overlooked, and later come back to cause havoc for your organization. With that said, methods that organizations, as well as individuals, can utilize so their data isn't affected or stolen include identifying and classifying their data. This method can be done by having a data discovery technology scan your system and return their finding to you. This will help you identify what type of data you have, where they belong, and how to get to them. It can also show you any alerts or any information that is stored in the incorrect place. Having knowledge of where all your data is kept can significantly reduce the chances of it being leaked or misused. A program like Netwrix Data classification makes this task so much easier to complete. Another method that can aid in protecting your data is having an Access Control List. This allows you to be able to see every person who has access to your data, the level of restriction, as well as every single time they access the data. This can display information about the people potentially trying to access your data, who may not have the proper access, as well as cover you for any instances of employee sabotage. In situations where an ex-employee may leave an organization on a sour note, the employee can hold a grudge against their previous employer, and try to use their access

level to leak information, but having an Access Control List offers you the ability to see all those who access your system and possibly even prevent disasters before they happen. The usage of data encryption can also significantly aid in protecting data because it allows data to be secured even if someone with unauthorized access somehow gains an opening into a security system. Encrypting data on portable devices is just as important because this allows the information to be safe while not connected to the main system, Using a program such as Encrypting File Systems (EFS) on Windows is a great way to secure your data and prevent leaks and losses. BitLocker is another great encryption tool that can help in securing data because it provides an additional layer of protection on top of EFS, especially against theft because it can provide secure data disposal if a system is compromised or no longer in use. Another great option to utilize when preventing data loss is definitely hiring an ethical hacker. Ethical hackers are usually hired to do penetration testing on the security of a system. They are highly certified and knowledgable individuals who will research, perform tests on a system, then provide their findings to their employers, as well as offer a course of action to better protect a system from malicious hackers and attacks. Ethical hackers are even a great option for those who are not digital natives as they can run security tests and implement changes that will last and provide a sense of security for their employers.

CONCLUSION

Data loss prevention is true of the utmost importance in today's society due to our constant usage and incorporation of technology into our daily lives. It is important that data, whether it be in the hands of an individual or a company be heavily safeguarded because these data give insight into exactly who we are, our interests, our ideologies, and even our biases. Using methods such as identifying and classifying data, access control lists, using data encryption as well as hiring professionals to ethical hack and penetrate your security system is critical when securing and protecting data from falling into the wrong hands. Studying and analyzing past events of data losses can also provide insight as to what methods can be avoided or implemented to strengthen a system so those events do not repeat themselves. Our very usage of technology invites people who want to exploit or take advantage of us or our data, so being informed on topics such as data loss is extremely necessary, because our data is our life, and if we have no control over our data, then we have no control over our lives.

REFERENCES

Liu, S., & Kuhn, R. (2010). Data Loss Prevention. *IT Professional*, *12*(2), 10–13. https://doi.org/10.1109/mitp.2010.52

Jones, R. (2018, March 19). *This Time, Facebook Really Might Be Fucked*. Gizmodo; Gizmodo. https://gizmodo.com/this-time-facebook-really-might-be-fucked-1823885655

Trabelsi, S. (2019). Monitoring Leaked Confidential Data. *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. https://doi.org/10.1109/ntms.2019.8763811

Liu, L., De Vel, O., Han, Q.-L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397–1417. https://doi.org/10.1109/comst.2018.2800740

10 Best Practices Essential for Your Data Loss Prevention (DLP) Policy. (2019). Netwrix.com. https://blog.netwrix.com/2019/07/16/10-best-practices-essential-for-your-data-loss-prevention-dlp-policy/

The CISO's Guide to Data Loss Prevention: DLP Strategy Tips, Quick Wins, and Myths to Avoid. (2017). Digital Guardian. https://digitalguardian.com/blog/cisos-guide-data-loss-prevention-dlp-strategy-tips-quick-wins-and-myths-avoid

Tomoyoshi, Hiroshi, T., Takayuki, T., & Ryusuke Masuoka, H. (2010). Data Loss Prevention Technologies. *FUJITSU Sci. Tech. J*, *46*(1), 47–55. https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol46-1/paper13.pdf