Aidan Kresak

ENG-112

Robert Arnold

7/12/2023

Data Breaches in Information Technology

If you own an antivirus software like Norton Antivirus, chances are you might receive updates on any data breaches that may have happened. In fact, you may have been victim to a data breach once yourself. Data breaches have become ever more common as technology grows and expands due to ways of breaching data growing as well. This puts any personal data that a private company possesses at risk of being of being damaged, destroyed, or even sold for financial gain. With this in mind, The United States should divert more energy and resources into developing new software to help combat this clear and present threat of data breaches.

It has been very common in the last decade for companies to take their customers' data for research purposes. This extends from taking credit card numbers, health records, phone numbers, and even birth certificate information. This is extremely valuable information, and it is this sort of information that must not be infringed upon. However, it is because companies have this sort of information that data breaches happen in the first place. Once a hacker breaches the company's data system, they now have access to a gold mine's worth of information. This information can be sold on the black market for a good price. According to invisibly, the average health record sold on the black market is worth about $250 according to Imprivata (2021). Now imagine that but hundreds to thousands of records sold. At that point, selling people's information can be a ludicrous yet illegal trade. It also does not help to notice that data breaching is becoming more and more common. According to Deloitte (n.d), the number of stolen records increased between 2015 and 2020 increased by 4,379%. This means that data breaches are becoming more common and that more people are trying to take advantage of other people's information. The pool of information and statistics stemming from data breaches is nearly endless with each statistic as important as the next. Therefore, it makes it more critical that we successfully defend from data breaches more effectively and frequently.

In order for us to defend against these malicious hackers more effectively, this requires us to create new and improved forms of antivirus software. Antivirus software has been used for a long time in protecting data companies and their customers' information. These take in the forms of firewalls, anti-spyware, and anti-virus software. Unfortunately, these sorts of technologies have their weaknesses. In firewalls, their purpose is to protect from any unauthorized traffic that takes place. However, it does not protect malicious programs from being ran or installed. Therefore, the threat from a data breach occurring due to a backdoor unintentionally installed on a data system thanks to the malware is still present. There are also weaknesses in modern antiviruses as well. The major drawbacks antivirus software is that cannot completely protect from all viruses as well as protect from every single virus. Apost on geeks for geeks stated that if a virus with the purpose of breaching a data system attacks and the antivirus software does not recognize as that kind of software, the database is essentially left to the mercy of the hackers

(2022). That is why it is incredibly important that our country is always attempting to provide new and improved types of software meant to defend data systems. Our data is highly valuable and new and improved antivirus software's that defend against more types of viruses as well as stronger firewalls being created will help are data stay secure and ensure the integrity and reputation of a company that holds other peoples data for the sake of their own company activities.

Since data breaches have occurred many times over the past decade, companies affected by these attacks have been taking notes on how to further protect from these and have implemented new measures to ensure the security of their customers data. One such thing that companies are implementing is the use of two-factor authentication. Normal forms of authentication include just typing in a password to access a device. With two-factor authentication, extra steps are added to reinforce the security of what is being accessed. This may take the form of an eye retina scan, a fingerprint scan, or even voice recognition. This makes it significantly harder for hackers to intrude because now they need physical authentication of someone to access any data. Therefore, the data system is now more secure thanks to extra layers of authentication required to access the data system and is very effective at what it was created to do. Companies at risk of their customers' data being exposed have also taken other measures like constantly updating their data system's security system. A data system security system that is constantly being updated allow for it to stay in top shape. Failing to consistently update the security system allows for the data system to be more vulnerable to an attack thanks to the fact that its defense is weaker than it should be.

In addition to these defenses, Zero-trust models of security, according to Endpoint protector have been adopted across many companies to further their defense against data breaches. In this model, any sort of traffic that occurs on the network is considered as untrusted and requires a resources to be verified and secured (2021). Since hackers attempting to breach data systems has to participate in traffic on the data network to breach it in most cases. Zero trust models are highly effective in defending against data breaches. This model can be thought of as the mindset of trusting no one to protect yourself from others hurting you. Lastly, in the scenario where all of these defenses fail and the data system is breached, companies have begun to practice encrypting their customers data when they obtain it. What this does is that this makes the information unable to be decrypted unless a digital key is used. Therefore, a hacker can obtain this data by breaching the system but they are unable to use this data thanks to not having the key to decrypt it. This makes all of the effort in breaching the data system be all for naught and they turn up with information they cannot even use.

These methods that have been stated above have been around for quite some time and have been proven to be useful. Unfortunately, this does not mean that they absolutely perfect. Hackers are always finding new ways to penetrate data systems that exist outside of the defenses that would normally work. This is largely thanks the fact that the internet is always changing and things that take place on the web constantly become more sophisticated. The fact that data breaches have occurred in the first place is proof that the internet is constantly evolving along with the fact they are constantly becoming more sophisticated and difficult to attack. This is why more time and resources should be focused on providing for improved and new types of software involved in defending against data breaches. The companies in possession of our data are taking every possible measure that they have in their arsenal to ensure that our data is protected so that both sides of companies and customers benefit. Data is valuable enough as it is, and we should be doing everything that we can to help provide backup to these companies with our support for new governmental action. Unfortunately, these data breaches have been on the rise for the past few years and our current efforts do not seem to be reversing the trend. It can not be stressed enough about how valuable our personal data is and the integrity of that data should be protected at all costs. Hackers can do unspeakable things with our data like commit identity theft by using credit cards for themselves or by destroying important health information about a certain individual who had a disorder. By focusing our resources into developing new and improved software, we shall protect the data that companies hold of us from being stolen by another and we will be able to live our lives without the fear of someone interfering with our normal life.

References

Imprivata. (2021, June 30). *Hackers, breaches, and the value of healthcare data.* Imprivata. Retrieved from https://www.imprivata.com/blog/healthcare-data-new-prize-hackers#

Deloitte. (n.d). *The growing threat of data breaches.* Deloitte. Retrieved from https://www2.deloitte.com/ca/en/pages/risk/articles/growing-threat-of-data-breaches.html

Coos, Andrada. (2022, April 11). *5 Ways Large Enterprises Protect their Data.* Endpoint Protector. Retrieved from https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/

Vanshgaur14866. (2022, August 2). *Anti-Virus; Its Benefits and Drawbacks.* Geeks for Geeks. Retrieved from https://www.geeksforgeeks.org/anti-virus-its-benefits-and-drawbacks/#

Coos, Andrada. (2021, July 12). *The First Steps Towards Zero Trust Security.* Endpoint Protector. Retrieved from https://www.endpointprotector.com/blog/the-first-steps-towards-zero-trust-security/