Opinion: Human Error is the Biggest Risk in Cybersecurity

December 8th, 2021

Introduction

Being safe and the feeling of being safe are two completely different ideas. It is easy for humans to feel safe. Just seeing an antivirus program, security cameras or a person standing near the front door can give a sense of security. I believe many companies nowadays sell the feeling of security rather than security itself. All it takes is a criminal to figure this out and that sense of security can be taken away with one action. A company with limited resources should have a reasonable balance between the training of personnel and additional security technology. With technology becoming smarter, humans are becoming the weaker part of the spectrum.

Criminals are starting to target the mind rather than the computer. It is of utmost importance for a company to have firewalls, secure cloud connections, backup servers/data, 24/7 monitoring, antivirus, and more. Without this, the company would be easily accessible by intruders, and the CEO may as well say goodbye. These measures ensure that both company and private data are secure and no one not authorized to do so can access that information. Security measures build trust with clientele and lighten the risk of profit loss as well. However, no matter how much money may be dumped into security technology, all it takes is one human to make a mistake and compromise the entire database.

The Human Factor

Humans have become the easiest straightforward access point into a company. With enough manipulation, a criminal could get wherever they want just by sending fake emails, lying, or talking to someone. Think of how many scam calls someone may receive in a week. These scammers may be making a thousand calls a week, and it is definite that people not educated on this topic may fall for these scams. From here, the scammer could gain access to many things, including but not limited to their bank account, identity, work identification, or their company itself.

Phishing is one example of human error causing cyber-damage, but that is not the extent of this topic. Within a company, there are advanced cyber security systems put in place to ensure no one unauthorized is able to access their information. While setting up these systems, there is an enormous amount of room for human error. Some programs, networks, or systems may be forgotten or disregarded, leaving an open port for a threat.

Although rare, insider criminal activity is also a real threat that may affect many businesses. An individual may have malicious intent themselves or could have been paid by an outside source to access private company data or perform malicious actions to their systems. A company should always have security systems in place for their own employees and monitoring for out-of-place actions.

One may ask themselves, “How does a company stay safe from both human and technological error while being accessible, accountable, and quick?” There are many resources and models for companies and individuals to follow to ensure the safety of the individuals and their systems. For example, the CIA Triad is a business organization model used to keep a company safe, while still accessible. Additionally, the NIST Framework is another model used by individuals to build a cybersecurity department and respond to certain threats accordingly.

The CIA Triad

The CIA Triad is almost a requirement for businesses to follow in order to create an effective cybersecurity department. There is not exactly a point when it was created, nor who created it, but it was more of a joint effort over the decades put together into one format. The CIA does not stand for the Central Intelligence Agency, but it is an acronym for confidentiality, integrity, and availability. When storing information digitally, these three words are of the utmost importance.

One’s data should always be stored confidentially. To do this, many systems may have one or multiple ways to authenticate and authorize each user accessing the data. To authenticate the user, the system may require something simple as a password or keycard, or it can be as complicated as a fingerprint or retina scanner. Even though the user may be authenticated, that does not mean they are authorized to have access to all of the information. That is the difference between authentication and authorization. Many systems will allow the user to log in and authenticate, but it will not authorize all of the files depending on their security clearance.

The integrity of data is vital to the security of a system's information and its trustworthiness. When transferring data, it should stay the same way it was and the data should be correct. Think of a cash register at the local grocery store. A customer comes up and buys an item for $5, the system accounts for tax and displays the final total to the customer before they pay. This way, the customer trusts the system and knows it holds integrity. It should always be able to prove to the user that the data stayed correct.

At last, the data system should have good availability for users trying to access it. Authenticated users may have important documents they need to access in an instant, but there is no point in having the data in that system if it is not available. One of the greatest traits about the Internet of Things is that it is available at all times, no matter where you are (with proper connection and accessibility, of course). The internet is the biggest data storage system out there, holding every single website, piece of information, video, music, or anything else one may decide to store digitally. All systems should compare and try their best to be as accessible as that.

All things considered, the CIA Triad is an incredibly important model to ensure that digitally stored data is safe, secure, and accessible. It is always up to interpretation based on the company's or individual's needs, but it should be compared closely and wisely.

The NIST Framework

Organizations can use the NIST Cybersecurity Framework and gain many benefits from using it. The framework lays everything out for an organization to keep its company secure and safe from outside hackers trying to break it. They can refer to the framework for many of their needs, and it can be used for training purposes (even for the average non-cyber security worker) to keep themselves safe. Every business is different and with that, different risks will show themselves; however, the framework generalizes many risks and the companies can still use this and edit it to their needs if needed. When I am in the cybersecurity field, I can see myself using this framework on a daily basis to organize and manage any cybersecurity risks that come my way. It will be a good guide until I know what to do from memory. The best part about the NIST Framework is that, like cybersecurity itself, it always changes. It'll update as needed to stay the most reliable for workers around the world.

Conclusion

In conclusion, no matter how much smart technology is implemented into a system to protect it, humans are always the ones behind it and there is always room for error. Whether it is malicious scammers manipulating people for their information, leaving a password unprotected, or leaving a port open, there is always one way or another for someone to break into a secure database. Although inevitable, there are tools available to lower the probability of human error, including the CIA Triad and the NIST Framework. Businesses and individuals alike should use these tools to ensure the safety of their information and to stray attackers away.

References

Fruhlinger, J. (n.d.). The CIA Triad: Definition, Components, and Examples. https://drive.google.com/file/d/1Mn3icTLG5X3W7tJjuDaohW8OscHdLOQI/view

Election security spotlight – CIA triad. CIS. (2021, June 15). https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

Cyberbitsetc. (n.d.). *Cyberbitsetc - why is cyber security about human behavior?* Cyberbitsetc.org. https://docs.google.com/document/d/1QplIrfcKImkSOuKt9i0Kte72kYrukFeCm1wj9DxpnGU/edit

National Institute of Standards and Technology . (n.d.). *Framework for Improving Critical Infrastructure Cybersecurity*. Google Drive. https://drive.google.com/file/d/1wPp9kofp-gdIu3NAisszeM8d8ko1djF1/view