

Name: Chase Seider

Date: 11/20/22

The Human Factor

The Human Factor plays a major role in the security of company data and systems. The strongest security systems and programs in the world are made and maintained by humans. One thing that every single human does during their lifetime is make mistakes. It's these mistakes that allow attackers to get past even the strongest security.

Social Engineering

Social Engineering is when attackers try to trick someone to give them information or allow them access to a system they should not have access to. In a perfect world where everyone was educated on Social Engineering and what to do and what to not do, this would not be an issue. But we are all Human and part of the Human Factor is that we all make mistakes. This was evident in the WannaCry ransomware attack that happened in 2017. This ransomware affected hundreds of thousands of windows computers across the world. This ransomware encrypted your system until it for the money it was asking for. Microsoft had issued a patch to stop the ransomware vulnerability but there were many organizations that failed to update their windows systems. Because of this the ransomware was able to spread long after it was patched.

Limited budget and cybersecurity training.

Not all organizations have unlimited funds to throw at training programs and cybersecurity protections. Because people will always make mistakes and there will always be attackers crying to capitalize on those mistakes, my budget would treat each means of cybersecurity as important as the other. Half of my budget would go towards training programs for employees to teach about the dangers of social engineering and what they should do to keep them and the organization safe. The other half would go towards more sophisticated cybersecurity protections.

Conclusion

In conclusion, humans are always going to make mistakes and those mistakes will lead to cyber threats and attacks. Even the strongest cybersecurity protections are vulnerable to being bypassed by an unsuspecting employee giving out information or allowing access to the wrong person. The Human Factor is a very important piece of cybersecurity and companies should realize the importance of educating their employees on how to stay safe and aware from making these mistakes.

References

The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from

Within. (n.d.). Kaspersky. Retrieved November 21, 2022, from

<https://www.kaspersky.com/blog/the-human-factor-in-it-security/>

Rosencrance, L. (n.d.). *What is WannaCry Ransomware?* TechTarget. Retrieved November 21,

2022, from <https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware>