Name: Hannah Johnson

Course: CYSE 200T

Data: November 8, 2024

The Human Factor in Cybersecurity

BLUF

The chief Information security officer has a lot of responsibilities and duties that they oversee to ensure the safety of the company's resources (CISCO, 2022). A limited budget poses certain problems that could arise if it was not allocated with utmost consideration and foresight to the different needs and aspects of the company. A CISO needs to ensure that funds are distributed in a way that fully protects the company and prepares it for potential incidents.

Evaluation of current security system

Before putting in all of the work to try and change a system, it is important to take inventory of what parts of that system are working and what parts could be improved upon or are failing entirely. One way that this could be done is to conduct a risk assessment. This in a sense is almost like an all encompassing gauge by which you can easily tell where your security is strongest and where the gaps are. By doing this you can find where you might be able to back down on some of the systems and then where to use that extra revenue to enhance the weaker spots, leaving you with a holistic security system.

Prioritize training

A really important yet sometimes overlooked part of cybersecurity is employee training. Sometimes especially when the budget is tight, this can be overlooked because on the surface it

doesn't necessarily seem like it would be the modest effective aspect, but human errors are actually some of the weakest areas when it comes to cybersecurity. Not only can this help employees to be aware of phishing attempts or other common malware incidents, but it can also enable them to help make informed decisions about security in their specific field (Simeonov, 2024) This one expense can end up growing exponentially to create a culture of cybersecurity in the workforce and overall mitigate many future attacks (Simeonov, 2024).

Technology and detection investments

While having prepared employees is very important and extremely helpful to preventing cyber attacks, humans certainly can't foresee or detect every instance of threat actors. This is why it is important to integrate technological detection and security measures. An example of this would be endpoint protection or EPP. EPP is a system that works on devices that are remotely connected to other devices and ensures that they follow compliance standards (Endpoint Security, 2024) . It works to block file-based malware attacks, identify malicious activity, and deliver the investigative and remediation tools required to address evolving security incidents and alerts on such devices (Endpoint Security, 2024). Another helpful technological tool is security information and event management, or SIEM. SIEM works to organize, detect, and respond to possible cyber threats before they can cause damage to the organization (What is SIEM, 2024). This system streamlines the detection process by automating what was once a manual system into an easy to use, detection and responses program (What is SIEM, 2024).

Conclusion

Prioritizing the security of a company can become really difficult when dealing with budgeting issues. It is tempting to be lax on some protocols to be able to spend that money in another area that might be just as useful. But when it comes to keeping information safe, a company has an obligation to its customers and employees to do everything in its power to ensure the protection of its assets. Some effective ways a CISO can do this that will be beneficial in the long run are implementing training to prepare employees and having security and detection systems running at all times so that an attack will not be likely to surprise you. Possible one of the most important parts however, is having an even coverage of security in all areas. Allowing just one access point to an intelligent attacker can spell the end to a company.

References

Cisco. (2022, December 7). *What is a Ciso? chief information security officer*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-ciso.html#:~:text=A%20CISO%2C%20or%20chief%20information,policies%20to%20protect%20critical%20data.

Endpoint security. Wikipedia. (2024, October 21). https://en.wikipedia.org/wiki/Endpoint_security#:~:text=An%20endpoint%20protection%20platform%20(EPP,dynamic%20security%20incidents%20and%20alerts.

Ibm. (2024, September 11). *What is Siem?*. IBM. https://www.ibm.com/topics/siem

Simeonov, M. (2024, July 12). *Proactive cybersecurity & the cost of cybersecurity training*. AMATAS. https://amatas.com/blog/proactive-cybersecurity-why-training-is-the-best-investment-you-can-make/