Name: Hans Peterson

Date: 3/24/2024

Human Factor in Cybersecurity

With limited funds, as a CISO, I would invest in training programs, cybersecurity software, and redundancy options.

Training Programs

The first option I would invest in, given limited resources, would be training programs. According to Security Awareness Training Statistics and Trends (2022), “85% of data breaches were due to the ‘human element.’” These data breaches can result in millions of dollars in damages, and they can impact a company’s reputation, driving customers and shareholders away. Employees need to be resilient against phishing attacks since these cyberattacks are abundant, and employees are often targets. To instill awareness, employees will undergo live-fire practice to refine their skills. However, since not all employees have the same level of awareness/skill, training is personalized for each employee.

Cybersecurity Software

The second option I would invest in is cybersecurity software, such as antivirus, IDS, IPS, and firewalls. It is the second layer of defense in case the human element fails. Antiviruses can recognize malware and quarantine it. According to Fortinet (2023), “IDS solutions excel in monitoring network traffic and detecting anomalous activity.” IDS software provides an extra layer of defense alongside human monitoring. Firewalls can block certain insecure ports (Ex. Telnet) and websites.

Redundancy

The final option I would invest in is redundancy. Specifically, I would invest in cloud storage, hard drives, RAID, and even cold sites. According to Awan (2023), “Redundancy ensures an alternate path or backup system is ready to take over seamlessly if one essential network component, such as routers, switches, or internet connections, fails.” This continuity ensures that systems continue to operate, reducing potential losses from downtime. Cold sites are able to continue operations at the cost of time. Data should be backed up on hard drives.

Conclusion

Training programs, cybersecurity software, and redundancy are the three options I would invest in if I were CISO. Training employees increases their resilience against phishing attacks and potentially prevents data breaches. Investing in cybersecurity software, such as antivirus and IDS, grants an extra layer of security. Investing in redundancy protects data and allows businesses’ systems to operate with little downtime and loss.

References

Awan, H. (2023). *A Comprehensive Guide on Network Redundancy: Its Benefits, Risks, and Best Practices*. Www.efani.com. https://www.efani.com/blog/what-is-network-redundancy

Fortinet. (2023). *What is an Intrusion Detection System (IDS)?* Fortinet. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

Security Awareness Training Statistics and Trends. (2022). Security Mentor, Inc. https://www.securitymentor.com/security-awareness-training-statistics-and-trends