Emerald Valadez 11-1-2024

CYSE 200T

Professor Kirkpatrick

The Human Factor in Cybersecurity

As a Chief Information Security Officer, employee training would be the priority because it helps address the root cause of many breaches involving human error. After having a strong foundation with training, technology would follow, focusing on the tools that provide the most value, such as firewalls, endpoint protection, and MFA.

Employees are often the weakest line of defense against cyber-attacks. According to a study by IBM, human error is the main cause of 95% of cyber security breaches. In other words, if human error was somehow eliminated entirely, 19 out of 20 cyber breaches may not have taken place (Ahola, 2022). Educating your employees on security basics and best practices allows them to make better decisions and enables them to keep security in their mind and seek further guidance when they're not sure what the consequences of a certain action are.

The remaining budget will be strategically allocated to the most critical technologies that strengthen our overall security posture, focusing on firewalls, endpoint protection, and multi-factor authentication (MFA). Firewalls keep an eye on attempts by unwanted traffic to access your client's operating system. They form barriers between computers and other networks (Rouse, 2022). Adopting a firewall for your client's security infrastructure helps set up their network with specific policies blocking or allowing traffic (Rouse, 2022) Also, endpoint security software enables businesses to protect devices that employees use for work purposes or servers that are either on a network or in the cloud from cyber threats. Endpoints are often the primary targets of attacks, such as ransomware or cryptocurrency mining threats or entry points for advanced, multi-stage attacks. As organizational workforces become more mobile and users connect to internal resources from off-premises endpoints, the vulnerability of these endpoints increases significantly (What is Endpoint Security). Out of the 93% of company networks that were penetrated, only 14% had endpoint protection solutions in place. Finally, MFA is critical. Passwords can leave organizations highly vulnerable to a breach, with more than 80% of hacking-related security breaches involving stolen credentials per the Verizon Data Breach Investigations Report. And as businesses increasingly move toward cloud-based and SaaS solutions and tools such as single sign-on (SSO), compromised credentials pose an even greater threat, as a single password can be exploited to gain access to all applications and systems within an organization's cloud-hosted environment (Mersch, 2021). Together, firewalls, endpoint protection, and MFA, form the foundation of a robust, multi-layered security strategy that helps mitigate risk and defend against emerging cyber threats.

Cybersecurity awareness training empowers employees with the knowledge and skills needed to recognize and respond to online threats, significantly reducing the likelihood of a successful attack. More importantly, it fosters a culture where every team member understands their role in maintaining the organization's overall security posture. While robust technological defenses are essential, even the most advanced systems can be compromised if an attacker successfully deceives an employee. Therefore, my primary focus would be on strengthening the human element through comprehensive training. Technology would then follow training. Ensuring we have strong firewalls in place, endpoint protection, and MFA. All these together would create a strong, well-rounded cybersecurity foundation.

References

Ahola, M. (2022, June 17). *The role of human error in successful cyber security breaches*. usecure Blog. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Mersch, A. (2021a, October 11). *Why multi-factor authentication (MFA) is a must-have for your business*. Prosource. https://blog.totalprosource.com/multi-factor-authentication-business-cybersecurity

Rouse, G. (2024, April 16). *What is a firewall and why is it important in cyber security?*. Datto. https://www.datto.com/blog/what-is-a-firewall-and-why-is-it-important-in-cyber-security/

What is endpoint security?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-security