## Initial Post

When designing secure infrastructures and networks, the understanding of the threats your systems are exposed to are crucial. Appropriate preventative, detective, and corrective controls are put in place to limit systems’ attack surface. Malicious attackers, typically motivated by recognition, greed, or power, exploit various attack vectors to achieve their goals. Organizations must deploy network and software security technologies to mitigate attacks from external agents, as well as people within the organization.

IT staff are trusted with elevated privileges to various systems depending on their role – servers, databases, endpoints, etc. These accounts are called privileged accounts. Privileged Identity Management (PIM) solutions allow organizations to manage, restrict, and audit identities with elevated privileges. The primary weakness of credentials, usernames and passwords, is the human element (Cobia, 2019). Easy to guess usernames, weak passwords, and regular accounts being assigned elevated rights leaves organizations vulnerable to credential theft which can lead to further loss depending on an account’s privileges. Retail store Target experienced a massive data breach in 2013 when a third-party vendor, who was granted remote access to various Target’s finance systems, fell prey to a phishing attack leading to compromised credentials (ibid.). This breach could have been averted if Target or its third-party vendor employed PIM policies and solutions to separate privileged accounts and manage their credentials. Users requiring elevated rights to perform a task (e.g. run a PowerShell script) or access sensitive data should request access to do so through a PIM solution which can follow an approval workflow prior to being granted access.

Honeypots are a popular security mechanism deployed to keep attackers away from an organization’s legitimate network. A honeypot is a “sweet” opportunity for an attacker to exploit intentionally configured pseudo-flaws of a computer (e.g. unpatched systems). Honeynets serve the same purpose as honeypots, instead are equipped with multiple computers with possibly different vulnerabilities. In addition to keeping malicious agents away from your organization’s legitimate network, honeypots enable security teams to analyze an attacker’s attack vector and gather information on the source of the intruder. Honeypots can also aid in identifying zero-day exploits. Honeypots should only be used to entice attackers. Openly advertising honeypots in hopes to induce an attack and charge the attacker is a form of entrapment, which can be used as a legal defense in a court of law (Walde and Flanagan, 2003).

References:

Cobia, Anea. “Privileged Access Management.” *La Salle University Digital Commons*, 15 Feb. 2019, digitalcommons.lasalle.edu/ecf\_capstones/34. Accessed 3 Oct. 2021.

Walde, Dr. Ian, and Anne Flanagan. “Honeypots: A Sticky Legal Landscape?” *Nexis*, 1 Jan. 2003, advance.lexis.com/document/?pdmfid=1519360&crid=2039dde9-d1fa-479c-8aaa-fba497715fa1&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A49NG-WX60-00CT-S0C4-00000-00&pdcontentcomponentid=152490&pdteaserkey=sr0&pditab=allpods&ecomp=ybxnk&earg=sr0&prid=9aa6f65d-4a38-4700-90b1-b2155968b5cf. Accessed 3 Oct. 2021.

# Summary Post

Organizations must utilize security techniques, tools, and processes (TTPs) to protect data confidentiality, integrity, and availability (CIA).  Network and software technologies are implemented to protect against internal and external threats. As perfectly articulated by Chan. (2021), when designing security solutions, it’s imperative that there is a balance between security and convenience. Additionally, controls in place should comply with legal and regulatory requirements to ensure security efforts aren’t squandered when dealing with a breach.

To protect your network from malicious attackers, honeypots can act as a decoy resource, to distract attackers from compromising your legitimate network. The use of honeypots can be traced back to the Cold War. A West German attacker was attempting to steal data from what seemed like a production US government computer system but was in fact an early incarnation of a honeypot setup by computer systems expert, Clifford Stoll, to entice hackers (Greene, 2021). Today honeypots and honeynets are incorporated in the deception technology security technology, powered by machine learning and artificial intelligence (ibid.). They allow security teams to keep attackers away from their production environment, perform detailed analysis of attackers’ source and hacking strategies, and gather intelligence on zero-day threats.

Balakrishnan. (2021) identifies two related yet distinct components within Identity Access Management (IAM) technologies – Identity Management and Access Management. Privileged Identity Management (PAM) solution is a software technology also within the IAM realm. Privileged identities include root, domain administrator, local administrator, and even business user accounts granted elevated rights. Such accounts must be managed, restricted, and audited through a PIM solution. PIM helps shift focus towards least privilege, and help minimize privilege creep, password sharing, and static credentials.

To conclude, network and software technologies like honeypots and PIM aid organization’s in their endeavours to strengthen their security posture and protect the confidentiality, integrity, and availability of data.

References:

Balakrishnan, J., 2021. *Collaborative Learning Discussion 2*. [online] Available at: [Accessed 30 August 2021].

Chan, Y., 2021. *Collaborative Learning Discussion 2*. [online] Available at: [Accessed 30 August 2021].

Greene, J. M. (2021) ‘Honeypot (computing)’, *Salem Press Encyclopedia*. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=ers&AN=149996227&site=eds-live (Accessed: 6 October 2021).