Name: John Ryan

Date: February 12, 2023

The CIA Triad

The CIA triad is the cornerstone of cybersecurity and many technical means exist to protect each of its elements. The processes of authentication, authorization, and accounting are essential in its maintenance. The DIE triad's take on CIA focuses on the impact of both security measures and security events to the business.

Confidentiality

Chai (2022) defines confidentiality as "roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts (p. 1)." Confidentiality ensures that sensitive information, such as PII, trade secrets, and national security secrets remain restricted to those who have the need to know.

There are many technical solutions available, often deployed in depth, to protect confidentiality. Encryption of data-at-rest (e.g. disk encryption), data-in-motion (e.g. TLS), and data-in-use (e.g. virtualization-based security) protect sensitive data. Data loss prevention systems detect the exfiltration of the same. Access control mechanisms prevent unauthorized access at the host or file level.

Integrity

“Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle (Chai, 2022, pp. 1-2).” Alteration of data itself can cause harm. An altered digital bank ledger would have obvious consequences. However, compromise in the integrity of files is a more insidious threat. Distribution of malicious code posing as legitimate system files remains an effective method of attack for hackers.

File integrity monitoring programs (e.g. AIDE), hashing algorithms (e.g. SHA), and checksums all provide technical means to protect integrity.

Availability

Ensuring availability “means information should be consistently and readily accessible for authorized parties (Chai, 2022, p. 2).” Availability is simply the ability to conduct business as usual, with all systems and data available to employees, customers, and other stakeholders.

Failover clustering, database mirroring, host backups, load balancers, RAID, and redundant power all protect availability.

Authentication, Authorization, and Accounting

Understanding authentication, authorization, and accounting, commonly referred to as AAA or Triple-A, is essential for protecting CIA.

Authentication is the process by which a user’s identity is proven. The three factors of authentication are: something you know (e.g. a password or PIN), something you have (e.g. a token), and something you are (e.g. fingerprint, iris, or retina). There are additional factors that can be tested at the time of authentication, such as location (somewhere you are), to further

prove identity. Multifactor authentication, increasingly the standard for information systems (Joint Task Force, 2020, pp. 132-133), is the use of two or more of the above factors concurrently. Establishing identity is critical, not only in the following step of authorization, but also for non-repudiation (Joint Task Force, 2020, pp. 132).

Authorization is the process of granting a user access once authentication is complete. This is accomplished using a tiered access model (Walsh et al., 2023), access control lists (ACLs), and file permissions. Control may be implemented through mandatory access control (MAC) or discretionary access control (DAC). MAC is administrator-controlled (e.g. SELinux), while DAC is at the discretion of the resource owner (e.g. NTFS permissions on a user-created file).

Accounting is the process of logging the use of an information system. Any compromise to CIA will require investigation of these logs, and having established identity at authentication, the principal of non-repudiation prevents an individual denying responsibility.

The AAA process of a user accessing a system would start with the user offering an identity by providing a username or certificate on a token. These would be checked against an identity provider solution like Active Directory. The user would present their password or PIN, respectively, and be authenticated. Attempts at accessing resources locally or on the network would be tested against whatever applicable rules are in place, the user restricted to accessing only those assets required to do their jobs (the principal of least privilege). All of this can be logged for later review.

Beyond CIA

There are advocates for a transition of the CIA triad into what is deemed a more business-focused framework: the DIE model of distributed, immutable, and ephemeral systems. This new

model maps to the triad, with ephemeral data protecting confidentiality, distributed systems availability, and immutable systems integrity.

According to Yu (2022), distributed systems prevent dependence on a single system, immutable assets are impossible to change, and ephemeral assets have a short and defined lifespan (para. 5). In the “pets” versus “cattle” analogy, the goal is to make as many assets as possible into the less-cherished, disposable cattle class, “mak[ing] them as low in value as possible through designing them to be DIE so that even if they are vulnerable, the impact is not worth the effort it takes to fully secure them (Yu, 2002, para. 7).”

The DIE model complements the push towards DevOps and infrastructure-as-code (IaC) methodologies—that is, a focus on fast-paced deployment and replaceability. Broken or compromised systems may be jettisoned and quickly spun up from a secure baseline.

Conclusion

The CIA triad remains the core goal of cybersecurity and security professionals continue to develop methods and tools to work towards this goal. Controlling user access through AAA methods is a requisite piece of any cyber security program. The DIE model offers an expansion on the CIA triad, one seeking to respect security without burdening the organization. Impact mitigation is valued over the overhead of protecting too many critical assets.

References

Chai, W. (2022, June 28). *What is the CIA Triad? Definition, Explanation, Examples.* TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Joint Task Force. (2020, December 10). *NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Mathers, B., Wahl, S., Tillman, M., Neira, B., Gremban, K., Baldwin M., & Poggemeyer, L. (2023, February 8). *Tier model for partitioning administrative privileges.* Microsoft. https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

Yu, S. (2022, March 15). *The Dept. of Know Live!: Sounil Yu on why embracing the DIE security model means faster innovation.* Fastly. https://www.fastly.com/blog/the-dept-of-know-live-sounil-yu-on-why-embracing-the-die-security-model-means-faster-innovation