Security, Access, and the CIA Cybersecurity Model

Nathan A Park

Old Dominion University

Course Number: CYSE200 - 17364

Professor Charles E. Kirkpatrick

Due Date: 9/17/23

Table of Contents

Security, Access, and the CIA Cybersecurity Model

The CIA Triad is a model used to help information security groups prioritize and target efforts to protect an organization's data. Confidentiality, integrity, and availability make up the core tenets of the model and use authentication and authorization as key components. Authentication is the confirmation of identity, while authorization, being dependent on authentication, refers to the rights granted to a user or entity within a system (Technology N. I., n.d.).

Authentication and Authorization

It is best to explore the definitions of authentication and authorization as well as their relationship as they are used throughout the CIA model. Authentication is the process of verifying a user's identity and is accomplished by using an intrinsic and unique property of the user such as their knowledge, possessions, or physical characteristics (Technologies, 2023). Passwords, personal datapoints, biometrics, and physical keys are some examples of items used to verify identity (Technologies, 2023). Knowing who has access to data, systems, and resources contributes to information security by providing traceability and accountability.

Authorization cannot occur without authentication and is essential to controlling an organization's resources (Technology N. I., 2006). Knowing who is allowed to do what helps determine when a breach of security has occurred. For example, a former human resources employee at a company will likely still have account data used to verify their identity but no longer has authorization to view personnel files like performance reviews or payroll. The National Institute of Standards and Technology alone has several definitions for authorization,

however, most essentially deal with the rights or official sanction to perform a function or use a resource (Technology N. I., 2006). These rights can be based on roles within an organization or specific attributes about a user or system (Technologies, 2023). For example, the finance department at a company might use an expense tracking application that is not available to users from other departments and certainly not accessible to the outside world. An example of attribute-based authorization is the use of public library computers where they are made available to users only during certain hours.

Confidentiality

Confidentiality deals with the privacy or secrecy of information (Chai, 2023). Only certain entities should have access to sensitive information since the unauthorized release of such data could have serious consequences ranging from identity theft to damage to national defense.

Clearly, secrecy cannot be maintained without first authorizing users. Confidentiality limits access to those who have a legitimate need and must cover storage, access, and transmission of data. It may not be appropriate to use offsite storage for some forms of data, transmission and storage likely need encryption, and employees might require background checks and training.

Integrity

Integrity deals with the authenticity of data. This means that only authorized alterations should be made including preventing accidental changes (Chai, 2023). Loss of integrity can seriously impact operations. Compromised quality assurance data might cause rejection of a

product. The corruption of a database can waste thousands of man hours in recovery and reconstruction efforts.

Administrative tactics and technologies are used to enforce integrity. For example, maintaining redundant copies, using mathematical techniques for tamper indication, and logging all accesses made to a resource are recommended practices (Chai, 2023). If a breach is suspected, auditable records can help forensic analysis teams trace the source and take measures to prevent future events. Authentication and authorization are useful tools as well. Knowing who can access and change information creates a chain of custody for accountability purposes. Put simply, organizations need to know when changes occurred and who made them.

Availability

Availability is the idea that desired information and resources are available to an authorized user within a reasonable time (Kim & Solomon, 2018). Availability can be affected by targeted attacks or system failures and requires mitigating measures based on the importance of the information. In industrial settings for example, a SCADA (supervisory control and data acquisition) system must be highly available. This can be accomplished using redundant communication paths, independent synchronized computing clusters, and multiple operating locations. Disaster recovery is also important to availability as organizations need to have a plan to restore from probable worst case scenario outages.

Availability is complex because users often require a minimum availability to accomplish tasks and prefer maximum freedom and flexibility for convenience. At the same time, the risks associated with exposing sensitive information to more access freedoms may be unacceptable.

The previously mentioned SCADA system might need to be placed behind a data diode to enforce limited one-way communication out of the network thus forcing vendors and technicians to travel to site for some evolutions.

Conclusion

In summary, the CIA triad, comprised of *confidentiality, integrity, and availability*, is about control of information because it covers who can access and change information and what level of accessibility is appropriate for authorized users. Furthermore, for each member of the triad, knowing who, authentication, is allowed to do what, authorization, is essential to protecting data. By focusing policy on these tenets, organizations efficiently use limited resources to prevent security breaches. Any organization, whether a company, government office, or one person operation, will have unique requirements and risk profiles and can use the CIA triad to create policies that best meet their needs.

References

Chai, W. (2023, February). *What is the CIA triad (confidentiality, integrity, availability)?* Retrieved from techtarget.com: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security.* Burlington, MA: Jones & Bartlett Learning.

Technologies, S. (2023, March 3). *What is the difference between authentication and authorization?* Retrieved September 15, 2023, from Sailpoint: https://www.sailpoint.com/identity-library/difference-between-authentication-and-authorization/

Technology, N. I. (2006). Minimum Security Requirements for Federal Information and Information Systems. *Federal Information Processing Standards Publications (FIPS PUBS 200)*.

Technology, N. I. (n.d.). *Computer Security Resource Center*. Retrieved September 16, 2023, from NIST: https://csrc.nist.gov/glossary/term/security_authorization