Principles of Information Security Assignment

Mohanad Horani

University of Advancing Technology

Security Essentials

Principle #1: There is No Such Thing as Absolute Security- In other words, the first principle of security is stating how there is always room for improvement in terms of security and how no organization is perfect in terms of their security. Also, determined hackers will continue to find new methods in weakening organizations in terms of their security. Some examples of how this can occur include exploits, insider threats, poor staffing, and insecure hardware (BlackPoint Cyber, 2019). A practical example of how to implement the first principle is to update hardware and software every week or month or hire new staff if required to complete the task.

Principle #2: The Three Security Goals are Confidentiality, Integrity, and Availability- In other words, confidentiality is denying access that is not authorized, integrity means to keeping data how it is, and availability means making data more accessible for use with authorized permission (Fenwick, 2014). This is also known as the CIA triad. A practical example of how to implement this includes utilizing secure passwords to protect data or utilizing password managers. Another example would be allowing some information that is not private available for the public.

Figure 1- https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/

Principle #3: Defense in Depth as Strategy- The third principle is discussing layered security measures (Fenwick, 2014). For example, if one security implementation fails, then there is

another that is available for use. There are also three elements to protect data from being accessed which are prevention, detection, and response (Fenwick, 2014). An practical example of this is the fact that networks which have security have routers, firewalls, and intrusion detection systems (Breithaupt & Merkow, 2014) to block the network from possible intruders. Phishing is another example of how people can be tricked into giving out personal information.

Principle #4: When Left on Their Own, People Tend to Make the Worst Security Decisions- In other words, this principle states that people fall for scams more easily and attempt shortcuts when left on their own (Fenwick, 2014). An example of how this could possibly occur is when someone is convinced to give away their credentials in exchange for a trivial item (Breithaupt & Merkow, 2014). A way to prevent this is to install antiviruses and also be cautious about who receives your personal identifiable information. In addition, working with an organization that knows more about the topic of cybersecurity is beneficial as well.

Principle #5: Computer Security Depends on Two Types of Requirements: Functional and Assurance- This principle states that functional requirements explain what a system must do and assurance requirements explain how a functional requirement should be enforced and tried (Fenwick, 2014). In other words, verification and validation are an alternative way to describe such a principle as well (Breithaupt & Merkow). An example of how this could be implemented is car safety testing. Verification testing for seat belts includes performing stress tests on fabric. The validation part (also known as the assurance testing) means that the seat belt needs to be verified to be safe and proven to be used under normal conditions. As of for software, verification can include beta testing a version for Apple or Android for bugs and security issues.

Principle #6: Security Through Obscurity is Not an Answer- This includes the fact that details of the security mechanism never is sufficient in protecting a system. One reason for that includes

that if the secret is out, the entire system is breached as a result. A solution for this is to ensure that multiple mechanisms are responsible for security, not only one (Fenwick, 2014). In other words, if someone discovers how something works, the entire system is at risk and someone can easily unveil these secrets as well. A practical example of this is leaking information about a new product when not necessary.

Principle #7- Security = Risk Management: This principle is stating that evaluating the risk and allotting the resources accordingly will protect against security threats. It also states that security is not only about removing all threats but also about minimizing losses if there is a successful attack launched by a hacker. In addition, risk analysis/management are key components in securing systems as well. Also, in real life, risk management is much more complex than only making a judgement based on human instinct or previous experience. It is crucial to realize the specific type of data the system maintains as well as what hardware/software will be utilized and the skillset of the development teams (Breithaupt & Merkow, 2014). A practical example of when to utilize this principle is if a security breach is announced ahead of time. That way, risk management techniques can be applied before the security breach even occurs.

Principle #8- The Three Types of Security Controls are Preventative, Detective, and Responsive: This principle states how security controls should contain mechanisms in order to prevent loss of data from occurring. In other words, countermeasures or controls should each serve a purpose by detecting whether or not there is a security breach or even responding to a breach when it is happening or after it has been revealed. For example, when a bank is being attacked, there are motion sensors as well as alarm systems in order to detect any unusual activity so the proper authorities can be notified as well (Breithaupt & Merkow, 2014).

Principle #9- Complexity is the Enemy of Security: This principle states how too much complexity in terms of a network or a system is never a smart idea and only will allow implementation of security more complex in the long run as a result. In other words, the system that is being secured will become more difficult to secure as a result. For example, if an organization has extremely complex security measures then even the organization will forget what is occurring in terms of their security and data.

Principle #10- The tenth principle of security is explaining how trying to force upper management into spending money on security is not a good method in obtaining resources. Instead, communication by explaining what is required and the reason for it is a much easier method in obtaining such resources. In other words, communication is key. Otherwise, the management of any organization related to security can deny such a request without proper justification. An example of this is forcing someone to upgrade their desktop by using fear tactics and demands.

Principle #11- The eleventh principle is stating how people are need in order to utilize the processes/technology in order to make a system more secure (Fenwick, 2014). For instance, it takes a person in order to install the latest software update or to configure a firewall for a computer (Fenwick, 2014). Without people to find technical problems, computer systems would not even exist or operate properly. Putting all hope in technology is never the right way to think since people fix technology frequently. Overall, people and technology work hand in hand.

Principle #12- The last principle states how disclosure of vulnerabilities is permissible. In other words, it is permissible to let users know about patches and fixes. Not letting users realize what issues there are is extremely bad for businesses (Fenwick, 2014). An example of this is reporting bugs with software upgrades that are in beta and relaying them to upper management by any

means necessary. Without relaying such information, some businesses do not even realize what needs to be fixed for the next version or upgrade. This also relates to Principle 6 of security as well (Breithaupt & Merkow, 2014).

References

12 Cyber Security Principles From The Experts: Blackpoint Blog. (2019, February 6). Retrieved January 19, 2020, from https://blackpointcyber.com/blog/12-cyber-security-principles/

Breithaupt, J., & Merkow, M. S. (2014, July 4). Pearson IT Certification. Retrieved January 19, 2020, from http://www.pearsonitcertification.com/articles/article.aspx?p=2218577

Fenwick, T. L. (2014, December 13). Twelve Information Security Principles of Success. Retrieved January 19, 2020, from https://ezinearticles.com/?Twelve-Information-Security-Principles-of-Success&id=8846855

The Three Goals of Cyber Security-CIA Triad Defined. (2019, August 29). Retrieved January 19, 2020, from https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/