Security Policies

These policies will be based around the 12 Principles of Information Security (Mark S. Merkow, 2014). We will have an executive summary as well as a practical example of how each principle could be implemented within a typical organization.

Principle 1

Nothing will every be secure no matter how much security is in place. Given enough resources, any security measure is as simple to break through like a padlock is with bolt cutters. We will do everything we can to prevent, detect, and respond to any security threat that may happen.

Principle 2

Our goals will be to maintain confidentiality, preserve integrity, and promote the availability of data to authorized users. This is known as the CIA triad.

Confidentiality is to make sure that nobody has access to data or information they do not need access to. This is done so that information will only be available to those who need it. There is no reason that an employee in sales needs access to any information that is in the HR department.

Integrity is kept so that any information and data will always be consistent. It also is to prevent any users from making any modifications to any data that are not authorized by upper management. It also helps keep mistakes from happening in databases where sensitive data is stored.

Availability models keep data accessible to those who are authorized for the data. This is especially important when any sort of disaster or emergency happens. If an earthquake hits your city and your office collapses, having data stored off-site keeps the data safe and still available to anybody who needs it.

Principle 3

Security will always need to be kept in layers, specifically prevention, detection, and response. Having defense in depth as a strategy works well for most security applications. Let us take a bank for example, more specifically, the safe inside the bank. Prevention would be the bank doors and guards. They are there to prevent any robbers from trying to get into the safe and steal the goods in there. Detection would be cameras, motion sensors, noise sensors, and any tripwires in the safe to detect if there is any unusual activity going in inside. Response would be any security measure that activates after something has been detected. Usually it is an alarm, but there can also be a lock inside the safe that trigger to make sure the safe stays closed until someone comes to investigate the alarms.

Principle 4

People tend to make bad choices, especially in security. One example of this is phishing emails. Phishing attacks are malicious attacks on companies or individuals to gain access into any sort of account they can. They are usually emails sent to you to look like other companies' emails. An example would be an attacker sending you an email that looks exactly like Instagram's. Everything looks exactly like how Instagram would send it except for the email address used to send it. They are meant to scare you into thinking your account has been hacked, accessed, or deleted so you panic and click a link that looks like a real link but instead they take you somewhere that looks like Instagram's websites. They will have you log into your account and as soon as you do that, they will get you. You have just given them your login credentials and now they have access to your account.

These are easy to recognize once you learn what to look for. Three things to look out for are grammatical errors, URLs you do not recognize, and emails. Even with learning with what to look for, keep in mind attackers get better and better every day, so if you see any unusual emails, let someone know and ignore the email (Ellis, n.d.)

Principle 5

Any sort of newly designed system will need to be made sure that it is doing the right things and doing them the right way. This is where verification and validation comes in. The verification process is the process of confirming that one or more predetermined requirements or specifications are met. Validation then determines the correctness or quality of the mechanisms used to meet the needs (Mark S. Merkow, 2014).

How padlocks are made is a perfect example. Verification for the locks would include material and stress testing on the shackle, testing the locking mechanisms, and confirming that the lock fits in a certain application. Validation is then done to prove the locks work repeatedly under normal working conditions and kept locked under much harsher conditions.

Principle 6

It is logical to think that if nobody knows how something works, then it is much more secure than if everybody knows how it works. This is actually false. Hiding details of how something works, works only if it is impossible to break through that security. As soon as someone does break through, now everybody can know.

When security is open-source, people are able to collaborate much more than when they are barred from viewing a system. When people are allowed to view open-source systems, they can find any security flaws that others may have hidden and can report them to someone who knows how to fix it.

Principle 7

Security is always balanced with risk management. Risk management is the process of making decisions to reduce the amount of risk without diminishing the quality of what you are protecting. Risk is calculated by the probability of something happening to the consequences if something does happen. If it is rare that something happens and a low severity of consequence if it does happen, then it is a low priority. If it is almost certain that something will happen and is catastrophic that something will happen, then it is an extreme priority.

Theoretical risk management is completely different in the real world. Every system is completely unique with its design, so there are different security requirements and considerations needed for each system. Every system will have vulnerabilities, each vulnerability can have an exploit made for it, and each exploit is made by an attacker.

Principle 8

Controls and countermeasures must be put in place to assist the principle of defense in depth. These go along with what we talked about in principle 3.

Principle 9

Do not make a system more complex than it needs to be. The more complex it is, the more vulnerabilities can occur. Just like with any machine, the more moving parts there are, the harder it is to fix.

Principle 10

Fear does not work in securing a budget for any security measures. It used to be, but now it must be a solid business decision in order to acquire any resources. This will make it more difficult to acquire any resources for security, but you should be able to convince management about what needs to be protected and why it needs to be protected in order to not lose more money for recovering from a security breach.

Principle 11

In order to properly secure anything, you need to have three “pillars.” They are people, process, and technology. These are all equally important for any organization. People are there for the “human element,” to have a final say for any decisions. This way nothing is decided without a human decision. Processes are implemented so that different people can perform tasks the same way each time. Technology is in place to help automate any tedious task as well as help with both people and processes. All three help each other out and balance out how an organization’s security works.

Principle 12

In principle 6, we talked about how security through obscurity does not work. This also works in reverse. Letting people know as soon as a vulnerability is found helps keep people informed that there are security risks and to not use the service while it is being patched. Knowing about flaws is better than keeping them a secret until they can be fixed, so people can protect themselves.

Works Cited

Ellis, D. (n.d.). *7 Ways to Recognize a Phishing Email: Email Phishing Examples*. Retrieved from Security Metrics: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Mark S. Merkow, J. B. (2014). *Information Security: Principles and Practices, 2nd Edition.* Pearson IT Certification.

Zainab Alkhalil, C. H. (2021, March 9). *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. Retrieved from Frontiers: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full