SECURITY DESIGN PRINCIPLES

1. Asset (Data) Clarification

Asset Clarification helps organizations to secure assets (either data or resources) based on their level of sensitivity. It helps identify data that need a higher level of security and must be protected.

2. Understanding Attackers

With time, attackers are becoming smart and identifying new ways to attack businesses. Understand the motives behind their targeted attacks and what resources they might use to ensure a successful attack.

3. Find the Weakest Link

Determine the weakest link in your security architecture that may be vulnerable to attacks. They can be devices, resources, or even humans. Identify them and ensure a strong cyber defense posture in your organization.

4. Understand the Architecture

Understand your security architecture and make security policies, methods, and models that suit your organization. Identify what security controls and safeguards you need for your security posture and align them with your objectives.

5. Minimize Attack Surface Area

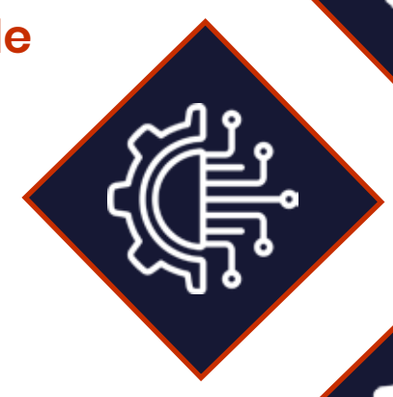
Minimizing attack surface area means removing parts of your system or software that you find vulnerable or insecure. These are areas where your system is the most vulnerable to cyber-attacks.

6. Establish Secure Defaults

The principle of secure default refers to setting the default configuration of your system restrictive to enforce conservative security policies. It means that, by default, the configuration is at the most secure settings possible.

7. Assign the least privilege possible

The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right.



8. Focus on Defense in Depth

Defense in depth means making a strategy leveraging various security controls to protect organization's assets. Focus on defense in depth so that if somehow defense is compromised, additional layers of security exist as a backup to stop threats.

9. Fail Securely

The principle of failing securely refers to the need to secure systems by recognizing the fact that security may fail. Even if failed security grants access to the systems, sensitive parts of your system will remain inaccessible.

10. Zero Trust

Today many businesses depend on third-party service providers for additional functionality and effective operations. Security by design ensures no user or application is trusted by default.

11. Separation of Duties

The idea behind the principle of Separation of Duties comes from the principle of least privilege. However, it is more focused on not giving too much authority to a single person. A person having too many permissions can become a liability in system security. Therefore, users must be given limited duties, so they don't fall apart and affect security operations.

12. Avoid Security by Obscurity

Security by Obscurity isn't an effective method as it focuses on hiding the details of security operations. It relies on the account's credentials remaining a secret. Users may gain access to those accounts over time. It is safer for companies to avoid this practice and implement effective security controls alongside.

13. Keep Security Simple

As IT environments become more complex, the solution to secure them is simple security. Keep Information Security simple to ensure everyone in the organization understands it and less time and effort are used to implement security.

14. Fix Security Issues Correctly

This principle focuses on the need to address security issues thoroughly and accurately to determine the root cause of the problem. Developers and system engineers must fix security issues correctly to minimize their recurrence.

15. Audit Sensitive Events

Auditing sensitive events will help organizations identify intrusion attempts and to determine the best possible way to reduce those events in the future.

ISAUnited
International Security Architects