CS-405

Talia Cunningham

8-2 Journal: Portfolio Reflection

* Adoption of a secure coding standard, and not leaving security to the end
  + In order to ensure the creation of secure and resilient software applications, it is crucial to implement a secure coding standard and incorporate security measures throughout the entire software development lifecycle (SDLC). This means that security considerations should not be left until the end of the development process, but should be integrated from the very beginning. By adopting such practices, developers can ensure that their applications are protected against potential security threats and can provide users with a safe and secure experience.
* Evaluation and assessment of risk and cost benefit of mitigation
  + When it comes to managing risks, evaluating and assessing them is an essential step. Organizations need to consider the potential costs and benefits of mitigation measures and compare them to the risks associated with a project or activity. By doing so, they can make informed decisions on which risks to prioritize and how to allocate resources efficiently. This process is crucial for ensuring that organizations can effectively manage risks and minimize the negative impact they can have on their operations.
* Zero trust
  + The concept of Zero Trust is a cybersecurity strategy and framework that is fundamentally rooted in the principle of not trusting any user, device, or system by default. This means that any entity that attempts to access resources, applications, or data, whether they are inside or outside an organization's network, must undergo continuous verification and authentication. The Zero Trust model requires this level of scrutiny regardless of the user's location or network connection. The key objectives of Zero Trust include bolstering security, mitigating insider threats, and shrinking the attack surface. This model is designed to provide an extra layer of security to organizations that cannot be breached by unauthorized entities, thus ensuring the protection of sensitive and confidential information.
* Implementation and recommendations of security policies
  + One of the most critical aspects of maintaining a secure organization is implementing and managing effective security policies. These policies are essential for protecting the assets, data, and systems that an organization relies on to function properly. Without proper security measures in place, an organization is vulnerable to a wide range of threats, including cyber attacks, data breaches, and other types of security breaches. Therefore, it is crucial to ensure that security policies are well-designed, regularly updated, and rigorously enforced to minimize the risk of security incidents and mitigate their potential impact.