John Brungard

CS405

10/17/2023

Module 8 Journal

* Adoption of a secure coding standard, and not leaving security to the end
  + A coding standard is a collection of rules, guidelines, and best practices to be taken by Software Developers when developing a program or application. Some examples of this include limiting the amount of each statement to 80-100 characters, naming conventions such as test classes starting with the name of the class they are testing and providing multi-line block comments for describing each function/class. Use of a Static Code Analyzer can ensure that your Coding Standards are being followed within the application.
  + Many popular and emerging methodologies such as Agile have begun practicing Test Driven Development in which code is tested in segments as they are completed. This can include Unit Tests, Integration, and Acceptance Testing. This is contrarily done to other models such as the Waterfall Method where testing is done after development.
  + We now look at the consequences of waiting to apply security at the end versus acting now and applying it during the earlier stages of the SDLC.
  + When we wait, it:
    - Can create a sense of distrust amongst clients due to loss or invasion of privacy.
    - May allow time for attackers to manipulate, steal, or delete important data.
    - Could create more cost in the repair of an attacked system.
  + When we act, it:
    - May prevent emerging or further damage of reputation involving your organization.
    - Mitigates any possible or future damage to the system.
    - Can save costs by testing and procedures compared to repairs.
* Evaluation and assessment of risk and cost benefit of mitigation
  + “Benefit-Cost Analysis (BCA) is a method that determines the future risk reduction benefits of a hazard mitigation project and compares those benefits to its costs. The result is a Benefit-Cost Ratio (BCR). A project is considered cost-effective when the BCR is 1.0 or greater.” (*Benefit-Cost analysis, 2023)*.
  + “Risk Assessment and Risk Mitigation is a process in which identifying, assessing, and mitigating risk takes place to scope, schedule, cost, and quality of the project." (GeeksforGeeks, 2022a).
* Zero trust
  + “Zero Trust is a significant departure from traditional network security which followed the “trust but verify” method. The traditional approach automatically trusted users and endpoints within the organization’s perimeter, putting the organization at risk from malicious internal actors and legitimate credentials taken over by malicious actors, allowing unauthorized and compromised accounts wide-reaching access once inside.” (CrowdStrike, 2023).
  + “Zero Trust is a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.” (CrowdStrike, 2023).
* Implementation and recommendations of security policies
  + Triple-A Framework
    - Authentication is the process of identifying the user trying to access the system. This can apply to user logins where a user supplies a username or password, and the system checks against those credentials.
    - Authorization is where the system determines the user’s level of access depending on their role within the system. An example of this are the available file access and privileges that an admin has on a website compared to a new user.
    - Accounting is the process of keeping documentation and accountability for the system and its data. This can include changes to the database and the addition of new users.
  + Encryption Policies
    - Encryption in rest refers to encrypted data that is not being used. An example of this is passwords in a database or other sensitive information that may not always be in use or hard drives.
    - Encryption at flight is the process of encrypting data that is leaving or entering a specific part of the application. An example of this is sending a message that uses asymmetric encryption.
    - Encryption in use is the encryption of security of data that is being used or accessed. An example of this is using a public key to decrypt a message.

References

CrowdStrike. (2023, April 17). What is Zero Trust Security? Principles of the Zero Trust Model. crowdstrike.com. <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

*Benefit-Cost analysis*. (2023, October 12). FEMA.gov. https://www.fema.gov/grants/tools/benefit-cost-analysis#:~:text=Benefit%2DCost%20Analysis%20(BCA),BCR%20is%201.0%20or%20greater.

GeeksforGeeks. (2022a). Short note on Risk Assessment and Risk Mitigation. *GeeksforGeeks*. https://www.geeksforgeeks.org/short-note-on-risk-assessment-and-risk-mitigation/