PORTFOLIO REFLECTION

Chase Carney

2/26/2023

It’s important that we pay close attention to the secure coding standards early on in the project. Bypassing this until the end can lead to greater problems for you and your team. This can include things like setting up permissions for users and only giving them the privileges that they will specifically need. Other practices such as defense in depth that uses the approach of ‘layering’ your security measures, gives you the best chance of detecting potential threats.

The cost of identifying and correcting defects in software grows significantly as time goes on in the software development process. Fixing bugs that are discovered after the software has been released can be extremely expensive and risky, generally costing significantly more than fixing them at earlier stages. Making changes to the code to fix a bug can also impact the functionality of the application, which may require additional changes to be made, increasing the cost, time, and effort required.

Things like one-time validation just don’t cut it because the threats and user attributes are all subject to change. It's important to continuously monitor and validate that a user and their device has the right privileges and attributes. To me it means that we should be taking a more 'hostile' approach at the way we look at current security approaches.

Here are some steps that should be taken in the implementation of security policies:

Acceptable Encryption and Key Management Policy.

Data Breach Response Policy.

Disaster Recovery Plan Policy.

Personnel Security Policy.

Data Backup Policy.

User Identification, Authentication, and Authorization Policy.

These are all important steps in the fight against attackers. Being prepared and knowing what to do if something were to slip through the ‘layers’ greatly increases the prevention of such attacks.