Dusten Schacht

6/18/2023

Project Two: Security Policy Presentation

Hello my name is Dusten Schacht and I will be explaining my security policy and why making sure that using the best security possible is always the correct thing, defense-in-depth is about having as many layers as possible to make sure that an attack cannot get access to the system as there will just be to many systems for the attack to go through, such as physical security, cloud security, perimeter security, network security, host security, endpoint security, app security, etc and you can also use automation to find coding vulnerabilities using unit tests and inputting things to see if you are able to break into the app yourself but you can also limit inputs using automation so that’s a different way of handing that type of situation, the ten coding standards are, validate input data, heed compiler warnings, architect and design for security policies, keep it simple, default deny, adhere to the last principle of least privilege, sanitize data sent to other systems, practice defense in depth, use effective quality assurance techniques, adopt a secure coding standard.

Encryption in rest means protecting data that is being stored, encryption in flight means to protect data that is moving, and encryption in use means to protect data that is being created or just used in general,