Introduction

Cybersecurity

Cybersecurity is a constantly moving target. New vulnerabilities are constantly being found and exploited. Increasing staff other people with access at organizations premises are going ‘stealth’ an attacking vulnerability's from within.

Unfortunately, Accenture (a company that provides technology consulting services) expect the costs of cybersecurity to grow exponentially in the future.

Standards

A standard is something that can be used to measure a level of quality. Standards often contain recommendations on how to attain such quality. Standards are used in IT to provide good practices that can benefit those who use them.

Standards are created by many independent organizations such as:

W3C – Who provide web standards

ISO – Who provide general information technology standards

The Open-Source Web Application Security Project

The goal of the OWASP project is to improve software security. OWSAP is formed of a number of independent partners such as Panasonic and Accenture.

OWASP has created a Security Knowledge Framework which helps those who apply it to create software that is better protected from hackers.

The OWASP Top Ten Pro-active controls is a list of security techniques OWASP believe should be considered for every project:

- C1: Define Security Requirements
- C2: Leverage Security Frameworks and Libraries
- C3: Secure Database Access
- C4: Encode and Escape Data

- C5: Validate All Inputs
- C6: Implement Digital Identity
- C7: Enforce Access Controls
- C8: Protect Data Everywhere
- C9: Implement Security Logging and Monitoring
- C10: Handle All Errors and Exceptions

OWASP has identified a number of weaknesses commonly found in software that include:

- Insufficient monitoring of system state
- Insufficient logging
- Broken access control
- Cross-site scripting

Insufficient monitoring of system state will mean that problems will not be identified until it much later and can cause greater damage.

Insufficient logging makes it harder to understand what went wrong if a problem occurs.

Broken access control allows users to perform actions they should not be able to.

Cross-site scripting allows malicious users to execute malicious code as if it was authenticated.

Integrating Security during Agile Development

An agile approach to software development allows developers to return to earlier stages of the cycle with greater ease than with a waterfall developmental approach.

Agile encourages only creating the minimum amount of documentation to aid the development.

Integrating Security during Waterfall Development

Waterfall development is a sequential approach where each phase can only be started once the previous is completed. Waterfall development is suitable for projects that are predictable. If a change occurs which affects a previous stage, then it can incur a significant cost.

The Spiral development approach is similar to Waterfall except it involves iterating through the planning, risk analysis engineering and evaluation phases until completion.

Scrum

The Scrum framework details how work can be broken into a 'backlog' of tasks that can then be completed in a series of sprints. After each sprint, progress is reviewed and a new selection of tasks is selected for the next sprint.

Paired Programming

In paired programming developers work in pairs during the coding process. One developer code while the other watches, then the pair switch roles. The person observing can gain understanding from the developer and also give feedback for the development.

Test-Driven Development (TDD)

TDD is a software development process where the tests are written before the production code.

UML

UML is used by software developers to depict systems. UML has a recognized syntax – a type of graphical language. UML diagrams help support communication with stakeholders.

UML diagrams can represent different views of the system, for example, the structure or behaviour of the system.

Structure diagrams present a static view of the system whereas a behaviour diagram presents a dynamic view.

Different types of MUL diagrams are suitable for different stages of the SDLC.

During the early stages of development use case diagrams can be used to help gather and capture requirements.

During the software design, class diagrams can be used to help design the structure of the system.

Sequence diagrams can be used to capture the information that flows between the classes.

UML models designed during development can be used to help later during the maintenance phase.