Aula TP - 08/Abr/2019

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 23/Abr/2018. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Exercícios

1. Risco

Como foi visto na aula passada, o objetivo do desenvolvimento de software seguro é reduzir o risco para níveis aceitáveis.

Relembre a fórmula de risco da aula passada:

> risco = probabilidade de ataque ter sucesso * impacto

em que

> probabilidade do ataque ter sucesso = nível da ameaça * grau de vulnerabilidade

Pergunta P1.1

Considere um PC doméstico e um servidor de *homebanking* de um Banco. Qual deles está está sujeito a um maior risco na Internet? Justifique, usando para tal a fórmula de cálculo de risco.

Experiência 1.1

Considere que a aplicação A de uma empresa tem o nível de risco R. Quais os fatores da fórmula do risco seriam afetados por:

1. Descoberta e encarceramento de cibercriminosos que ameaçavam a aplicação.
2. A empresa descobrir e remover diversas vulnerabilidades da aplicação.

2. Secure Software Development Lifecycle (S-SDLC)

Experiência 2.1

Em que fase do modelo em cascata deve ser levada em linha de conta o regulamento europeu RGPD?

Pergunta P2.1

Em que fase do modelo *Microsoft Security Development Lifecycle* deve ser levada em linha de conta o regulamento europeu RGPD?

Experiência 2.2

1. Em que função de negócio, prática de segurança e actividade do SAMM deve ser levada em linha de conta o regulamento europeu RGPD?
2. Em que nível de maturidade dessa prática de segurança tem de estar a empresa, para levar em conta o regulamento europeu RGPD nos seus projetos? Justifique.

Pergunta P2.2

Esta pergunta deve ser respondida pelos grupos com número par.

Em qualquer um dos S-SDLC é fundamental na fase de Requisitos identificar os requisitos de segurança, que devem ter por base a legislação em vigor e as recomendações e normas internacionais (família ISO 27000), conforme sejam aplicáveis, devendo ser traduzidos em requisitos específicos para o software a desenvolver.

O ISO/IEC 27002:2013 *Information technology -- Security techniques -- Code of practice for information security controls* fornece orientações para normas de segurança de informação e práticas de gestão de segurança de informação numa organização, incluindo a seleção, implementação e gestão de controlos de segurança, levando em consideração o ambiente de risco de segurança da informação da organização.

Analise os controlos de segurança indicados nas secções:

- 14.2 *Security in development and support processes*
- 10.1 *Cryptographic controls*

O que pode concluir em relação à utilização destes controlos no projeto de desenvolvimento de software que o seu grupo está a desenvolver para esta disciplina ou para outras disciplinas?

Nota: Pode encontrar o ISO/IEC 27002:2013 aqui.

Pergunta P2.3

Esta pergunta deve ser respondida pelos grupos com número ímpar.

O *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64, Security Considerations in the System Development Life Cycle*, foi desenvolvido para ajudar as Agências do Governo Federal dos EUA a integrar as componentes de segurança IT nos sistemas de desenvolvimento de ciclo de vida de software (SDLC) que utilizam.

Analise a secção 2.3 (*Key Roles and Responsibilities in the SDLC*). O que pode concluir em relação às funções e responsabilidades de segurança no SDLC, se comparar com os projetos de desenvolvimento de software em que tem participado?

Nota: Pode encontrar o NIST Special Publication (SP) 800-64 na diretoria Aula10.

3. SAMM (*Software Assurance Maturity Model*)

Nesta secção é-lhe pedido para utilizar o ciclo de melhoria contínua do SAMM, aplicada ao seu projeto da UC de Engenharia de Segurança.

Para isso deverá utilizar a Toolbox (ficheiro excel) fornecida na diretoria Aula10, onde também encontrará mais informação relativa ao SAMM.

Note que:

- Para a Fase *Assess* deverá preencher a *sheet* "*Interview*";
- Para a Fase *Set the Target*, o grupo deverá discutir qual o *score* objetivo das práticas de segurança identificadas. Se necessitar de pressupostos, indique-os na justificação à decisão tomada;
- Para a Fase *Define the Plan* deverá preencher a *sheet* "*Roadmap*", supondo que cada uma das fases tem 3 meses de duração. Tenha em conta o esforço necessário e a eventual dependência entre atividades em cada uma das fases.

Note que não há respostas certas nem erradas.

Pergunta P3.1

Identifique a maturidade de três práticas de segurança (à sua escolha) que utiliza no desenvolvimento do projeto da UC de Engenharia de Segurança (Fase *Assess* do SAMM)

Pergunta P3.2

Para cada uma das práticas de segurança identificadas na pergunta anterior, estabeleça o objetivo para a mesma (Fase *Set the Target* do SAMM), i.e., o nível de maturidade pretendido;

Pergunta P3.3

Desenvolva o plano para atingir o nível de maturidade pretendido identificado na pergunta anterior, em quatro fases (Fase *Define the Plan* do SAMM).