Aula TP - 16/Abr/2018

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.

Pergunta P1.2

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)

Pergunta P2.1

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

Pergunta P2.2.

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

Pergunta P2.3

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.

Experiência 2.1

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.

Experiência 2.2

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 Aula9.

Pergunta P2.4

Deve ser feita pelo grupo de projeto de desenvolvimento de software e foi adicionada uma nova secção (SAMM) ao projeto abaixo.

Projeto de desenvolvimento de software

Os alunos deverão utilizar o resto desta aula TP para continuarem o projeto de desenvolvimento de software.

O projeto 1 (Leilões online) será efetuado, em conjunto, pelos grupos 1, 6, 10, 11, 12.

O projeto 2 (Gestor de passwords com base em QrCodes) será efetuado, em conjunto, pelos grupos 2, 3, 4, 5, 7, 8, 9.

- Projeto 1 – Leilões online
  - Leilões online, com entrega de propostas em "carta fechada";
  - Pode ser uma extensão para software open source de leilões online.
- Projeto 2 – Gestor de passwords com base em QrCodes
  - Gestor de passwords, em que com base em QrCode apresentado pelo site, o telemóvel lê o QrCode e envia o user + password para desbloquear o acesso;
  - Pode ser uma extensão para software open source de gestão de passwords.

Nesta primeira fase, os dois grupos de projeto devem definir em traços gerais o projeto e as suas funcionalidades, e pensarem de que modo serão utilizado as técnicas criptográficas no projeto.

Como output desta fase, deverão ter um primeiro draft de:

- definição do projeto e suas funcionalidades,
- etapas e fluxos de comunicação / mensagens, podendo utilizar como exemplo o formato visto no segundo exemplo do voto eletrónico, na aula teórica. Esta componente deve conter um diagrama e uma parte textual de explicação do diagrama,
- identificar os passos efetuados para a concepção e desenvolvimento do projeto, de forma a seguir os princípios de "*privacy by design*" e "*data minimization*" do RGPD (Regulamento Geral de Proteção de Dados);
- identificar de que modo o software garante os direitos do titular dos dados, de acordo com o RGPD.

Estes pontos deverão fazer parte do relatório final do projeto.

SAMM (*Software Assurance Maturity Model*)

Nesta fase do projeto é-lhe pedido para, utilizando o ciclo de melhoria contínua do SAMM,

1. Avaliar a maturidade das práticas de segurança utilizadas no desenvolvimento de software deste projeto (Fase *Assess*);
2. Estabelecer o objetivo para cada uma das 12 práticas de segurança (Fase *Set the Target*), i.e., o nível de maturidade pretendido;
3. Desenvolver o plano para atingir o nível de maturidade pretendido, em quatro fases (Fase *Define the Plan*).

Para isso deverá utilizar a Toolbox (ficheiro excel) fornecida na diretoria Aula9, 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 para cada uma das 12 práticas de segurança, que sirva de guia para atuar sobre as atividades mais importantes. Pode partir do princípio que a sua organização é uma startup que vai efectuar desenvolvimento de software na área de i) sistemas web seguros online (caso do projeto 1) e ii) sistemas de identificação eletrónica (caso do projeto 2). Se necessitar de outros 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.

A Toolbox (ficheiro excel) deverá fazer parte do relatório final do projeto, fornecendo o ficheiro excel como anexo ao relatório. Adicionalmente, no documento do relatório deverá incorporar um anexo em que indique a decisão da Fase *Set the Target* e a justifique.

Note que não há respostas certas nem erradas.