Engenharia de Segurança

Aula 9 - 16/04/2018

Vulnerabilidades de codificação

Afonso Fontes (pg35389)

Bruno Carvalho (a67847)

Mariana Carvalho (a67635)

23 de Abril de 2018

Universidade do Minho

1 - Risco

Pergunta 1.1

Não é possível saber qual dos dois está sujeito a um maior risco na internet sem saber o nível de ameaça e grau de vulnerabilidade de cada um. Embora um PC doméstico em principio apresente uma maior probabilidade do ataque ter sucesso, pois provavelmente não é submetido a um control de segurança tão rigoroso como um servidor de *homebanking*, de qualquer das formas, um ataque a este último apresenta um impacto muito maior, sendo assim é extremamente provável que para valores de *probabilidade do ataque ter sucesso* a cima de zero em ambos os casos, o servidor de *homebanking* apresente um risco considerávelmente mais elevado.

Pergunta 1.2

Pergunta 1.2.1

O encarceramento de cibercriminosos que ameaçam uma aplicação faz com o nível de ameaça se torne mais baixo, influenciado por isso este fator na fórmula de risco.

Pergunta 1.2.2

Descobrir e remover vulnerabilidades da aplicação diminui o grau de vulnerabilidade da mesma.

2 - Secure Software Development Lifecycle

Pergunta 2.1

O RGPD deve ser tido em conta logo na Fase de Requisitos. No entanto, a implementação dos requisitos identificados em relação ao RGPD irá obviamente estender-se a todas as fases do projeto.

Pergunta 2.2

A regulamentação para proteção de dados deve ter sida em conta durante a fase de Requisitos do modelo *Microsoft Security Development Lifecycle*.

Pergunta 2.3

Pergunta 2.3.1

O regulamento europeu **RGPD** deve ser tomado em conta na prática de segurança *Policy Compliance* , uma prática respetiva à função de negócio *Governance*. Este regulamento deve ser levado em conta em fase inicial de levantamento de requisitos de segurança, pois são requisitos legais obrigatórios.

Pergunta 2.3.2

Pensamos que um nível um de maturidade seria suficiente para levar em conta o regulamento europeu RGPD nos seus projetos, pois o regulamento é criado de forma a ser facilmente compreensível sem haver necessidade de qualquer formação, no entanto, devido ao risco no incumprimento da implementação do regulamento, caso a empresa lide com grande quantidade de dados pessoais dos seus clientes, esta deveria garantir um nível 3 de maturidade no conjunto de atividades associadas a esta prática.