Aula 9 - 16 de abril de 2018

Grupo 8

1. Risco

Pergunta P1.1
De acordo com a fórmula de cálculo apresentada, podemos verificar que existem 3 fatores que influenciam o valor do risco: o nível da ameaça, o grau de vulnerabilidade e o impacto. Comparativamente a um servidor de *homebanking*, é menor o impacto de uma vulnerabilidade num PC doméstico, uma vez que, à partida, só é afectada uma pessoa, ao contrário do primeiro. Também o nível da ameaça é menor no caso do PC doméstico, devido ao valor que este contém em comparação com o primeiro. Tendo em conta a natureza sensível dos dados, o grau de vulnerabilidade do servidor será menor do que o do PC doméstico. Com isto, podemos concluir que é o servidor de *homebanking* que está mais vulnerável na Internet.

Pergunta P1.2
No cenário considerado, a descoberta e encarceramento de cibercriminosos que ameaçavam a aplicação diminui o nível da ameaça e, consequentemente, o risco. Já a descoberta e eliminação de diversas vulnerabilidades da aplicação por parte da empresa diminui o grau de vulnerabilidade e, consequentemente, o risco.

2. Secure Software Development Lifecycle (S-SDLC)

Pergunta P2.1
O regulamento europeu RGPD deve ser tido em conta na primeira fase do modelo Waterfall, a fase dos requisitos, de forma a que o software a ser desenvolvido cumpra as normas do contexto onde vai ser utilizado.

Pergunta P2.2
À semelhança do caso anterior, no modelo *Microsoft Security Development Lifecycle* o RGPD deve ser tido em conta na fase dos requisitos.

Pergunta P2.3

1. Como podemos observar pela tabela que se segue, o RGPD está presente em todas as funções de negócio do modelo SAMM:

2.

SAMM Domains		GDPR Articles
SM	Strategy & Metrics	5, 24, 32, 33
PC	Policy & Compliance	7, 24, 32, (12-21)
EG	Education & Guidance	37, 39
TA	Threat Assessment	25, 35
SR	Security Requirements	24, 28, 32
SA	Secure Architecture	25
DR	Design Review	24, 25, 30, 32
IR	Implementation Review	24, 25, 32
ST	Security Testing	24, 25, 32
IM	Issue Management	33, 34, 39
EH	Environment Hardening	25, 33
OE	Operational Enablement	32, 33

Ainda assim, a função de negócio principal é a de *Governance*. A prática de segurança *Policy & Compliance*, que se foca no cumprimento de requisitos legais externos assegurando, simultaneamente, que este cumprimento vai ao encontro das práticas da organização. Finalmente, a actividade particular é a *Identify and monitor external compliance drivers.*

2. Os níveis de maturidade são 4:
0 - Ponto inicial implícito que representa as actividades da prática.
1 - Entendimento inicial e provisão *adhoc* da prática de segurança.
2 - Aumento da eficiência e/ou eficácia da prática de segurança.
3 - Domínio da prática de segurança.

Podemos concluir que a empresa tem de estar no nível de maturidade 1, na fase inicial da prática, de forma a que o RGPD seja tido em conta desde o início do projecto.