Pergunta P1.1

Um PC doméstico de um utilizador normal, como não possui muita informação crítica, não está desenhado por defeito para suportar qualquer ataque realizado, estando apenas protegidos para ataques básicos. Comparando um servidor de *homebanking* de um Banco, que possui informação crítica de vários utilizadores, tem de estar mais preparado, em termos de segurança, de modo a aguentar a maioria dos ataques realizados a este. Sendo assim, o grau de vulnerabilidade de um PC doméstico é muito maior que o de um servidor de *homebanking* de um Banco.

Por outro lado, o nível de ameaça de um servidor de *homebanking* de um Banco é muito maior que o de um PC doméstico, visto que são alvos de vários grupos de atacantes, devido à informação que guardam.

Compare-se os dois valores que afetam a probabilidade de sucesso de um ataque. Dado a proteção atual dos computadores pessoais, juntamente com a emissão de atualizações periódicas, pode-se afirmar que a diferença, neste caso, entre o servidor de *homebanking* e o computador pessoal quase não afeta a probabilidade do ataque ter sucesso. No que toca ao nível da ameaça, pode-se afirmar que um servidor de *homebanking* apresenta um alvo com significativas maiores recompensas que o PC pessoal, apresentando assim uma maior probabilidade de risco para um servidor de *homebanking* de um Banco.

No entanto, o impacto do ataque é muito maior no caso do *homebanking* de um Banco, devido à informação crítica descoberta pelos atacantes, no caso de sucesso do seu ataque, ser muito mais valiosa que um ataque bem sucedido num PC doméstico.

Em conclusão, o risco de um servidor de *homebanking* de um Banco é maior que o de um PC doméstico.

Pergunta P1.2

1) Nível de ameaça diminui
2) Grau de vulnerabilidade diminui

Pergunta P2.1

O regulamento europeu RGPD deve ser levado em conta a partir da fase inicial de requisitos, minimizando a possibilidade de ocorrência de erros que tornem um *software* inseguro. Geralmente as práticas de segurança são implementadas em fases de teste, o que não é recomendado visto que muitos problemas podem nem vir a ser detectados.

Mais informação ver: https://www.synopsys.com/blogs/software-security/secure-sdlc/

Pergunta P2.2

Uma vez mais, apesar de não existir uma fase obrigatória para a implementação de requisitos que visam cumprir o regulamento RGPD, é recomendado que se leve em consideração os requisitos necessários para ser levantados na fase de levantamento de requisitos. Esta abordagem ajuda a identificar metas importantes, fornecendo informações úteis acerca de possíveis implementações e horários de entrega. Ajuda também a identificar possíveis metas mínimas de segurança que deverão ser implementadas, assim como resolver possíveis *bugs* que podem surgir.

Em suma, verifica-se que estas medidas de segurança (tanto em S-SDLC como MS DL) deverão ser implementadas, como recomendação, numa fase o mais inicial ao desenvolvimento do projeto possível, de forma a mitigar possíveis problemas futuros.

Mais informação ver: https://www.microsoft.com/en-us/sdl/default.aspx

Pergunta P2.3

1.

A RGPD deverá ser tomada em consideração na fase de negócio inicial, relativa a *Construction*. Isto ajuda a definir, atempadamente possíveis metas de segurança, que estarão contidas no *software* final, e possivelmente no *modus operandi* da própria empresa. Esta deverá, ainda, ser tomada em consideração nas práticas de segurança, na etapa de *Security Requirements*, garantindo que estes têm de ser implementados no projeto, e que devem ser ponderados e adicionados para fazer cumprir com o RGPD.

Atividades: *Assess*

Em que o objetivo é identificar e compreender a maturidade da organização em cada uma das 12 práticas de segurança, nesta fase utilizando a toolbox do SAMM serão avaliadas as práticas atuais e determinado o nível de maturidade.

2.

De acordo com o RGPD as práticas de segurança mencionadas devem-se encontrar no nível de maturidade 3 uma vez que este é o que se encontra de acordo com os requisitos de segurança definidos neste regulamento.

Mais informação ver:
https://www.hack2secure.com/blogs/summarizing-open-software-assurance-maturity-model-opensamm-requirements
https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Browse_Online