EXERCÍCIOS E ESTUDOS DE CASO

UNIDADE TEMÁTICA 1 - Introdução à Segurança da Informação

Este caderno contém exercícios práticos e estudos de caso desenhados para consolidar os conhecimentos adquiridos na Unidade Temática 1. Os cenários apresentados são inspirados em situações reais, com especial enfoque no contexto africano, visando preparar os estudantes para os desafios práticos da Segurança da Informação.

PARTE I: CONCEITOS FUNDAMENTAIS E TRÍADE CIA

Exercício 1: Identificação dos Pilares da Tríade CIA

Para cada um dos cenários abaixo, identifique qual pilar da Tríade CIA (Confidencialidade, Integridade ou Disponibilidade) foi comprometido e justifique a sua resposta.

1. Um funcionário de um hospital em Maputo envia acidentalmente um ficheiro Excel com os resultados de exames de 50 pacientes para uma lista de e-mail pública.
2. Durante o período de matrículas, o portal do estudante de uma universidade fica inacessível devido a um volume anormal de tráfego gerado por um ataque coordenado.
3. Um atacante consegue aceder à base de dados de um banco e altera o saldo da sua própria conta de 1.000 MT para 1.000.000 MT.
4. Um corte de energia prolongado na cidade da Beira desliga os servidores de uma empresa de logística que não possuía geradores de backup.

Exercício 2: Aplicação do Hexagrama de Parker

Considere o seguinte cenário: "Um gestor financeiro perde o seu computador portátil da empresa num táxi. O computador não tem palavra-passe de acesso e contém relatórios financeiros não encriptados."

Analise este incidente utilizando os seis elementos do Hexagrama de Parker (Confidencialidade, Integridade, Disponibilidade, Posse/Controlo, Autenticidade e Utilidade). Quais elementos foram violados?

PARTE II: AMEAÇAS, VULNERABILIDADES E RISCOS

Exercício 3: Classificação de Ameaças e Vulnerabilidades

Classifique os seguintes itens como Ameaça (A) ou Vulnerabilidade (V). Para as ameaças, indique a categoria (Natural, Humana Intencional, Humana Acidental, Tecnológica). Para as vulnerabilidades, indique o tipo (Técnica, Humana, Processual).

1. Falta de política de atualização de software na empresa.
2. Inundações sazonais que afetam o rés-do-chão onde se encontra o datacenter.
3. Um ex-funcionário descontente que ainda possui as credenciais de acesso ao sistema.
4. Utilizadores que escrevem as suas palavras-passe em post-its colados no monitor.

5. Um bug no código da aplicação web que permite injeção de SQL.

Exercício 4: Cálculo de Risco (Estudo de Caso Prático)

Uma instituição de microfinanças em Angola está a avaliar os seus riscos de segurança. Utilizando a fórmula RISCO = AMEAÇA × VULNERABILIDADE × IMPACTO, analise o seguinte cenário:

Cenário: A instituição utiliza um software de gestão de clientes desatualizado há 3 anos. Existe um grupo de cibercriminosos ativamente a explorar falhas nesse software específico na região. Se os dados dos clientes forem roubados, a instituição enfrentará multas severas e perda de confiança, podendo levar à falência.

Tarefa: Identifique claramente a Ameaça, a Vulnerabilidade e o Impacto neste cenário. Como gestor de SI, que medidas imediatas recomendaria para mitigar este risco?

PARTE III: ESTUDOS DE CASO - CONTEXTO AFRICANO

Estudo de Caso 1: O Ataque de Ransomware a Infraestruturas Críticas

Contexto: Em 2021, a Transnet, a empresa estatal de portos e caminhos-de-ferro da África do Sul, sofreu um ataque cibernético massivo. Os sistemas informáticos foram paralisados, forçando os portos a operar manualmente, o que causou atrasos significativos na cadeia de abastecimento de toda a região da África Austral. Os atacantes utilizaram uma variante de ransomware, exigindo pagamento para restaurar o acesso aos sistemas.

Questões para discussão:

1. Que tipo de malware foi utilizado neste ataque e qual é o seu principal objetivo?
2. Qual pilar da Tríade CIA foi o alvo principal deste ataque?
3. Discuta o impacto económico de um ataque deste tipo numa infraestrutura crítica para um país africano.
4. Que medidas preventivas (técnicas e processuais) a empresa poderia ter implementado para evitar ou minimizar o impacto deste incidente?

Estudo de Caso 2: A Ameaça do Mobile Money e Engenharia Social

Contexto: O Quénia é pioneiro mundial no uso de dinheiro móvel (M-Pesa). No entanto, com a proliferação destas carteiras digitais, aumentaram os crimes cibernéticos. Um esquema comum envolve criminosos que ligam para as vítimas fazendo-se passar por funcionários da operadora de telecomunicações (Safaricom). Eles informam a vítima que a sua conta está em risco de ser bloqueada e pedem que confirmem o seu PIN ou cliquem num link enviado por SMS para "verificar a identidade".

Questões para discussão:

1. Identifique e classifique as técnicas de Engenharia Social utilizadas neste cenário (ex: Vishing, Smishing, Phishing).
2. Por que razão a Engenharia Social é frequentemente mais bem-sucedida do que ataques puramente técnicos em plataformas de mobile money?
3. Como profissional de Sistemas de Informação, que campanha de consciencialização desenharia para proteger os utilizadores com baixos níveis de literacia digital contra estas ameaças?

Estudo de Caso 3: Vazamento de Dados Governamentais por Falha de Configuração

Contexto: Uma agência governamental num país da África Ocidental implementou um novo portal online para os cidadãos registarem os seus dados fiscais. Seis meses após o lançamento, investigadores de segurança descobriram que a base de dados na nuvem (cloud) que armazenava as informações estava configurada como "pública", sem qualquer exigência de autenticação. Milhares de registos contendo nomes, moradas e números de identificação fiscal ficaram expostos na internet.

Questões para discussão:

1. Este incidente foi causado por um ataque cibernético sofisticado ou por uma vulnerabilidade? Justifique.
2. Qual princípio da Segurança da Informação foi violado?
3. Qual é a diferença entre este tipo de incidente e uma violação de dados causada por um ataque de Man-in-the-Middle (MitM)?
4. Que controlos de segurança deveriam ter sido implementados antes do lançamento do portal?