QUESTIONÁRIO DE FIXAÇÃO 01

Aluno : Luan Brito Sousa Calazns 6°Sem - Teoric Analitic Cyber Sec

QUESTÃO 01

Assunto: Conceitos fundamentais da Segurança da Informação

Com base nos fundamentos da segurança da informação e considerando a necessidade de uma linguagem comum entre profissionais de diferentes áreas, defina de forma objetiva:

a) Segurança da informação;

A maneira com qual a mensagem é passada de maneira segura , integra , econfiavel , garantindo que nao passe por 3° , nem seja modificada durante a entrega

b) Incidente de segurança;

Pessoas que nao tem a capacidade de entender como a engenharia funciona , e acaba caindo em um truque (sendo inserindo um pen drive na maq , a descobrir informações pessoas durante uma conversa ''normal'')

c) Ativo;

Uma pessoa que conhece sobre engenharia pessoal , que sempre está em alerta , cuida do servidor sempre esta olhando arquivos de log , scaneando a rede , e garantindo a integridades dos dados

d) Ameaça;

Uma ameaça pode estar debaixo do seu nariz e voce nem fazer ideia , pode ser uma porta aberta , uma pessoa mal intencionada ,um funcionario nao bem intrucionado .

e) Vulnerabilidade;

Vulnerabilidade pode ser de uma porta de um serviço especifico ao firewall da rede , englobando engenharia e funcionarios que não são bons

f) Risco;

Risco que vc corre é de perder dados importantes como senhas de banco , ou arquivos compromentedores como videos pessoais com pessoas proximas , ou ate msm por uma falha em um BD onde o hacker pode até extorquir a pessoa em troca de ''devolver'' os dados ou deixar em ''paz'' aquelas vitimas

g) Ataque;

existe varios tipos de ataques , pode sera um servidor , a uma pessoa , um fishing de rede aberta (free wifi { email:senha }) , enegenharia social , analise de site (OSINT)

h) Impacto.

Uma vulnerabilidade pode fazer total diferença na sua vida ou ate msm na empresa que vc trabalha , podendo perder horas sem arquivos e perder dinheiro como consequencia e ainda pagar para ''receber de volta'' os seus dados.

Questão 02

Assunto: Conceito de Vulnerabilidade em Segurança da Informação

Durante uma reunião da equipe técnica da empresa *Delta Farma Digital*, especializada em prontuários eletrônicos, um analista júnior questionou o significado exato do termo **vulnerabilidade**, após o relatório de avaliação de riscos apontar que “vulnerabilidades críticas em endpoints expõem a rede corporativa a ataques de ransomware”.

Um dos gerentes pediu que cada membro da equipe explicasse com suas palavras o que entendia por **vulnerabilidade**, com o objetivo de nivelar o vocabulário técnico entre os setores.

Considerando os fundamentos da segurança da informação, **qual das definições a seguir mais se alinha ao conceito técnico de vulnerabilidade**?

C) É uma falha ou fraqueza que pode ser explorada por uma ameaça para causar dano.

Questão 03

Assunto: Propriedades de Segurança da Informação e Tipos de Ataque

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: **confidencialidade, integridade, disponibilidade e autenticidade**.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC 27001 e RFC 4949.

Situações apresentadas

I) Um disco rígido é fisicamente destruído após uma sabotagem interna.
II) Arquivos confidenciais são copiados por um usuário sem autorização.
III) Um funcionário malicioso altera dados de salário em uma planilha protegida. **IV)** Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

B) I–1 II–2 III–3 IV–4

Questão 04

Assunto: Classificação de ataques – ransomware e passividade/atividade

A equipe de segurança da empresa *NeoBank Digital* identificou um ataque de **ransomware** em seu ambiente corporativo. O código malicioso criptografou arquivos essenciais de clientes e servidores internos, impedindo o acesso às operações bancárias. O atacante exigiu pagamento em criptomoeda para fornecer a chave de descriptografia.

Durante o debriefing técnico, surgiu um debate entre analistas sobre a natureza do ataque: **teria sido um ataque passivo ou ativo?** Um dos analistas argumentou que não houve espionagem silenciosa, mas sim uma ação explícita com alto impacto operacional.

Com base na taxonomia de ataques em segurança da informação, analise as asserções a seguir:

I – O ataque de ransomware é classificado como um ataque ativo, pois altera o estado dos sistemas ou dados do alvo.
PORQUE
II – Em ataques ativos, o invasor interfere diretamente na integridade ou disponibilidade da informação, o que caracteriza o comportamento do ransomware.

A) As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da

I.

Questão 05

Assunto: Proteção da Confidencialidade da Informação

A confidencialidade é um dos pilares da segurança da informação e refere-se à **garantia de que o acesso à informação seja restrito apenas a pessoas,**

processos ou sistemas autorizados. No contexto corporativo, proteger a confidencialidade é essencial para preservar a privacidade de dados sensíveis, segredos comerciais, contratos estratégicos, informações de clientes e outros ativos de alto valor.

Incidentes de vazamento de informações, sejam por falhas técnicas, negligência humana ou má-fé, colocam em risco a reputação da organização, sua conformidade com legislações como a **LGPD**, e sua vantagem competitiva no mercado.

Explique, com base nas boas práticas de segurança da informação, **como uma organização pode proteger a confidencialidade dos seus ativos informacionais**. Em sua resposta, mencione **pelo menos dois tipos de controles aplicáveis (técnico, físico ou administrativo)** e **um exemplo prático de aplicação em ambiente real.**

R: Dar uma boa aula de boas praticas para os funcionarios , para não cairem em pishing mostrar um fishing para eles ao vivo como funciona ,
mostrar como espetar pendrivres até CD's Disket em computadores da empresa pode ser perigosos , Ter alguem que fique de olho no trafego do site na hora do pico de trafego da rede , tambem em horarios de lanche onde o firewall pode liberar alguma brecha
e tambem para se proteger contra ransomware vc pode fazer backups externos , em HD's backups programados para fazer ao 12:00/15:00/18:00; apagando o antepenultimo backup e salvando o penultimo assim podendo voltar qualquer coisa as definições do backup antigo.
Realizar simulações periódicas de incidentes ajuda a equipe a reagir rapidamente em caso de ataque real.

Questão 06

Assunto: Autenticidade e Integridade da Informação

Durante a construção de uma política de segurança da informação, uma organização buscou garantir que os dados mantidos em seus sistemas fossem confiáveis tanto em sua **origem** quanto em seu **conteúdo**. A equipe de segurança decidiu implementar **assinaturas digitais** em comunicações e

arquivos críticos, buscando preservar propriedades fundamentais como **autenticidade** e **integridade** da informação.

Contudo, parte da equipe demonstrou dúvidas sobre a diferença entre os dois conceitos e como se relacionam na prática da proteção de dados.

Analise as asserções a seguir:

I – A integridade da informação é garantida quando se assegura que os dados não foram alterados de forma indevida, intencional ou acidental.
PORQUE
II – A autenticidade da informação garante que os dados tenham origem legítima e possam ser atribuídos com confiança a uma fonte identificável.

B) As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.

Questão 07

Assunto: Classificação dos Modelos de Ataque em Segurança da Informação

Em um exercício de análise de ameaças, uma equipe de segurança foi desafiada a classificar seis eventos distintos segundo o modelo de ataque ao qual cada situação se refere, considerando a tipologia clássica: **interrupção**, **interceptação**, **modificação** e **fabricação**.

Situações analisadas

I) Adição de um registro falsificado em um banco de dados.
II) Desabilitar um sistema de arquivos.
III) Modificação de dados trafegando na rede.
IV) Inutilização física de um componente de hardware.
V) Captura de dados em rede, através de escutas.
VI) Alteração de um programa para que execute de modo diferente.

Associe corretamente cada situação ao seu **modelo de ataque**:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Assinale a alternativa que apresenta a **sequência correta para I, II, III, IV, V e VI**:

A) 4 – 1 – 3 – 1 – 2 – 3

Questão 08

Assunto: Identificação de vulnerabilidades em contextos organizacionais reais

Uma organização está realizando uma **análise de riscos informacionais** com foco na segurança física, lógica e organizacional. A equipe de governança foi instruída a identificar vulnerabilidades em diferentes frentes de atuação que, se exploradas, poderiam comprometer os ativos da informação — mesmo sem o uso direto de malwares ou técnicas avançadas.

Foram observadas quatro situações rotineiras, com potencial de exposição a riscos, e a equipe deve agora identificar **vulnerabilidades específicas que possam ser**

exploradas em cada caso, justificando suas análises conforme os princípios da segurança da informação.

Para cada uma das situações a seguir, identifique **uma possível vulnerabilidade explorável** e **justifique a resposta** com base nos conceitos de segurança da informação (disponibilidade, integridade, confidencialidade, autenticidade e rastreabilidade):

a) Pessoal de serviço diário de mensageiro realizando entrega e coleta de mensagens.

A) A pessoa pode modificar a integridade da mensagem ou até msm passar a informação para uma empresa inimiga , ou pais inimigo no caso de guerra .

b) Ex-funcionários que deixaram a empresa porque foram dispensados.

B) Pode deixar um backdoor (Camuflado) no servidor e apagar tudo de sacanagem com a empresa , ou fazer oque quiser vende informações , modificar e afins.

c) Funcionário viajando a serviço da organização e acessando a rede remotamente .

C) Alguem pode fazer uma analise no site da empresa e com essa analise descobrir o nome de usuarios da empresa obtendo Usuarios para brute force , depois descobrir o ip pelo DNS com ferramentas linux, e descobrir a porta 20/22/21 de ssh e executar um brute force de senhas e depois ja era

d) Utilização de notebook pessoal sem cadastro na lista de ativos.

D) Sinceramente nao sei , mas acredito que seja algo relacionado a nao identificar aquela pessoa que tem aquele remoto na rede ativa , podendo mudar configurações do wifi com o dispositivo remoto e fazer captura de dados.

Critério	**Peso**
Identificação correta da vulnerabilidade	40%
Justificativa coerente com os princípios da SI	40%
Clareza, objetividade e uso de vocabulário técnico	20%

Questão 09

Durante uma simulação de segurança em uma organização, cinco incidentes distintos foram observados. A equipe de resposta a incidentes foi orientada a classificá-los segundo os modelos clássicos de ataque: **interceptação**, **modificação**, **interrupção** e **fabricação (ou falsificação)**.

A análise correta dos incidentes é essencial para que os controles apropriados sejam implementados.

Com base nas situações descritas a seguir, identifique a classificação **mais adequada** para cada forma de ataque:

I) Um invasor acessa um arquivo transmitido de um cliente para um servidor sem autorização.

II) Um agente malicioso altera parte do conteúdo de uma mensagem em trânsito, sem interromper sua entrega.

III) Um sniffer é utilizado para analisar o tráfego de rede em tempo real.

IV) A rede torna-se inutilizável temporariamente devido a sobrecarga proposital de

tráfego.

V) Um atacante se passa por um usuário legítimo, utilizando suas credenciais reais.

Assinale a alternativa que apresenta a **associação correta entre as situações I a V e os modelos de ataque a seguir**:

1. Interceptação
2. Modificação
3. Interrupção
4. Fabricação (ou falsificação de identidade)

E) I–4, II–2, III–1, IV–3, V–1

Questão 10

Tema: Normas ABNT ISO/IEC da família 27000

A gestão da segurança da informação nas organizações depende da **adoção de boas práticas e diretrizes internacionalmente reconhecidas**. No Brasil, a ABNT adota e traduz as normas da família ISO/IEC 27000, que **padronizam processos, controles**
e estratégias para implantação e melhoria contínua de um SGSI (Sistema de Gestão de Segurança da Informação).

Essas normas têm escopos distintos, mas complementares — desde conceitos e vocabulários até requisitos e guias de implementação. O conhecimento dessas publicações é fundamental para profissionais da área garantirem conformidade, proteção de ativos e confiança organizacional.

Considerando as normas atualmente publicadas pela ABNT da família ISO/IEC 27000, assinale a alternativa que apresenta corretamente os **principais objetivos e características de cada uma das normas a seguir**:

- ABNT NBR ISO/IEC 27000
- ABNT NBR ISO/IEC 27001
- ABNT NBR ISO/IEC 27002
- ABNT NBR ISO/IEC 27005

C)

- 27000: Vocabulário e conceitos fundamentais para SGSI.
- 27001: Estabelece requisitos normativos para certificação do SGSI.
- 27002: Apresenta controles de segurança e boas práticas de implementação.
- 27005: Fornece diretrizes para gestão de riscos de segurança da informação.