Fundamentos de Cibersegurança

Nome: *Gabriel Domingues Silva* ***Turma:*** *24E3-5*

Tema: TP3

Prof. Fabiano Alves
Instituto Infnet

Conteúdo

1 Conceito de Segurança da Informação e seus Objetivos Principais

Segurança da Informação (SI) pode ser definida como o conjunto de práticas, políticas, procedimentos e controles destinados a proteger as informações de uma organização contra acessos não autorizados, modificações indevidas, divulgação inadequada ou destruição. Seus **objetivos principais** são geralmente resumidos nos princípios fundamentais conhecidos como a **tríade CIA** (*Confidentiality, Integrity, Availability*):

- **Confidencialidade:** Garantir que apenas pessoas ou sistemas autorizados possam acessar informações sensíveis.

- **Integridade:** Assegurar que os dados estejam completos e não tenham sido alterados ou corrompidos, intencional ou acidentalmente.
- **Disponibilidade:** Certificar que as informações e sistemas estejam acessíveis sempre que necessário, evitando interrupções nas operações.

Esses princípios são complementados por outros conceitos, como **autenticidade**, **responsabilidade** e **não repúdio**.

2 Impactos da Falta de Segurança da Informação

A ausência de medidas adequadas de SI pode trazer consequências graves, tanto financeiras quanto reputacionais para as organizações. Exemplos incluem:

- **Vazamento de dados:** Exposição de informações sensíveis, como dados financeiros, pessoais ou propriedade intelectual.
- **Perda de receita:** Interrupções em sistemas críticos podem levar à paralisação de operações.
- **Danos reputacionais:** A perda de confiança por parte de clientes, investidores ou parceiros pode impactar a continuidade dos negócios.
- **Multas e sanções legais:** Violações de legislações como a LGPD (Lei Geral de Proteção de Dados) ou o GDPR podem resultar em penalidades severas.

3 Importância de Políticas de Segurança da Informação

Quando uma pequena empresa lida com dados pessoais e expande suas operações sem uma política de SI, as consequências podem incluir:

- **Perda de dados:** Dados sensíveis de clientes podem ser comprometidos por ataques cibernéticos.
- **Repercussões legais:** Violações de privacidade podem resultar em processos legais.
- **Danos à confiança:** Clientes podem perder a confiança na empresa após o incidente.

Políticas de SI poderiam prevenir o incidente ao:

- Estabelecer controles de acesso robustos e senhas fortes.
- Implementar criptografia para proteger informações sensíveis.
- Realizar treinamentos regulares para conscientizar os funcionários sobre boas práticas de segurança.
- Monitorar e auditar os sistemas para identificar vulnerabilidades de forma proativa.

4 Exemplo de Comprometimento da Integridade dos Dados

A **integridade** dos dados é violada quando informações são modificadas de maneira não autorizada. Um exemplo seria:

> Em um banco de dados financeiro, um atacante insere transações fraudulentas ou altera valores de contas, causando prejuízos financeiros e dificultando a reconciliação.

5 Relação entre Segurança da Informação, Privacidade e Proteção de Dados

A **segurança da informação** fornece os meios para proteger a **privacidade** e garantir a **proteção de dados**, estabelecendo barreiras contra acessos indevidos. Essa relação pode ser descrita da seguinte maneira:

- **Segurança da Informação:** Abrange processos e ferramentas que asseguram os princípios da tríade CIA.
- **Privacidade:** Refere-se ao direito do indivíduo de controlar como suas informações pessoais são coletadas e usadas.
- **Proteção de Dados:** Inclui medidas específicas para garantir que informações pessoais sejam tratadas de acordo com legislações e padrões éticos.

6 Vulnerabilidades Humanas como Ameaças

Os seres humanos são frequentemente considerados o elo mais fraco na cadeia da segurança da informação. Exemplos incluem:

- **Erros humanos:** Configurações incorretas ou compartilhamento acidental de dados sensíveis.
- **Falta de conscientização:** Funcionários que clicam em links de *phishing*.
- **Descuido com senhas:** Uso de senhas fracas ou repetidas em múltiplos sistemas.

A mitigação dessas vulnerabilidades depende de programas contínuos de educação e conscientização em SI.

7 Impactos Potenciais da Falta de Medidas de Cibersegurança

No caso da startup de tecnologia:

- **Perda de propriedade intelectual:** Produtos ou soluções inovadoras podem ser roubados e utilizados por concorrentes.
- **Queda na competitividade:** A incapacidade de proteger seus ativos pode prejudicar o valor de mercado e a confiança de investidores.
- **Interrupção de negócios:** Ataques podem levar à paralisação das operações, afetando a sustentabilidade financeira.

8 Segurança da Informação Vai Além dos Dados Digitais

Embora frequentemente associada à proteção de dados digitais, a segurança da informação também inclui:

- **Informações físicas:** Documentos em papel, contratos e protótipos.
- **Comunicações:** Telefonemas e reuniões presenciais.
- **Infraestruturas críticas:** Proteção de sistemas de controle industrial e redes de energia.

9 Disponibilidade e Operação

A **indisponibilidade** de sistemas pode impactar severamente as operações de uma organização. Exemplos incluem:

- **Hospitais:** Falhas em sistemas podem atrasar diagnósticos e tratamentos.
- **Serviços financeiros:** Indisponibilidade de plataformas bancárias pode afetar transações.

10 Ameaças Mais Comuns

Entre as ameaças mais frequentes estão:

- **Phishing:** Tentativas de enganar usuários para roubar credenciais.
- **Malware:** Softwares maliciosos que comprometem sistemas.
- **Ransomware:** Sequestro de dados em troca de pagamento.

11 Ataques Cibernéticos

Tipo de Ataque	**Características Principais**
Phishing	Uso de e-mails ou mensagens fraudulentas para enganar usuários e roubar dados, muitas vezes levando-os a clicar em links maliciosos ou fornecer credenciais sensíveis.
DDoS (*Distributed Denial of Service*)	Envio de tráfego massivo e simultâneo de diversas máquinas para sobrecarregar servidores e torná-los indisponíveis, causando interrupções nos serviços.
Ataque de força bruta	Tentativa sistemática e automatizada de adivinhar senhas ou chaves criptográficas ao testar todas as combinações possíveis até encontrar a correta.

12 Ataque DDoS: Definição e Técnicas Relacionadas

Um **ataque DDoS** (*Distributed Denial of Service*) é uma tentativa maliciosa de tornar um servidor, serviço ou rede indisponível, sobrecarregando-o com um volume massivo de tráfego. Características principais incluem:

- **Origem distribuída:** O ataque utiliza múltiplas máquinas, muitas vezes controladas por uma botnet.
- **Objetivo:** Interromper operações legítimas ao consumir recursos do sistema.
- **Duração variável:** Pode durar minutos ou horas, dependendo da escala.

Outras técnicas de ataque que poderiam ser usadas no cenário descrito incluem:

- **Ataques de exploração de vulnerabilidades:** Injeção de códigos maliciosos em sistemas vulneráveis para comprometê-los.
- **Ransomware:** Sequestro de dados seguido de um pedido de resgate.
- **Phishing dirigido:** Tentativas de enganar funcionários-chave para obter acesso a credenciais sensíveis.

13 Conceito de "Ataque de Força Bruta"e Prevenção

O **ataque de força bruta** é uma técnica na qual um atacante tenta adivinhar credenciais ou chaves criptográficas por meio de tentativas sistemáticas de todas as combinações possíveis. Características principais incluem:

- **Natureza exaustiva:** O atacante testa inúmeras combinações até encontrar a correta.
- **Automatização:** Ferramentas automatizadas, como *Hydra* e *John the Ripper*, são frequentemente usadas.
- **Eficiência variável:** Depende da força da senha ou da chave a ser quebrada.

Medidas preventivas:

- **Política de senhas fortes:** Requerer combinações de letras, números e caracteres especiais.
- **Limitação de tentativas:** Bloquear contas após um número excessivo de tentativas falhas.
- **Autenticação multifator (MFA):** Adicionar uma camada extra de segurança além das senhas.

14 Tipos de Ataques à Rede

Tipo de Ataque	Características Principais

Sniffing	Captura de tráfego em uma rede para obter informações sensíveis, como senhas ou dados confidenciais.
Man-in-the-Middle (MitM)	O atacante intercepta e potencialmente altera a comunicação entre duas partes sem que elas percebam.
IP Spoofing	O atacante falsifica endereços IP para se passar por uma máquina confiável e obter acesso não autorizado.

15 Diferença entre Ataque Tecnológico e Não Tecnológico

- **Ataque Tecnológico:** Explora falhas em sistemas, redes ou softwares. Exemplos incluem ataques de malware, força bruta e DDoS.
- **Ataque Não Tecnológico:** Baseia-se na manipulação humana para obter acesso ou informações, como engenharia social e ataques de *phishing*.

16 Engenharia Social no Contexto da Segurança da Informação

A **engenharia social** refere-se à manipulação psicológica de pessoas para levá-las a realizar ações ou divulgar informações confidenciais. Exemplo típico:

- Um atacante finge ser do suporte técnico e convence um funcionário a compartilhar credenciais sensíveis.

17 Utilização de Informações Públicas em Ataques de Engenharia Social

Atacantes podem explorar informações disponíveis publicamente para planejar ataques, como:

- **Redes sociais:** Obter dados pessoais que facilitem a criação de mensagens de *phishing* personalizadas.
- **Sites corporativos:** Identificar hierarquias ou endereços de e-mail para simular comunicações internas legítimas.
- **Documentos públicos:** Descobrir detalhes sobre contratos ou fornecedores.

18 Treinamento para Prevenção de Engenharia Social

As organizações podem prevenir ataques de engenharia social ao:

- **Treinar funcionários:** Promover conscientização sobre práticas seguras, como verificar a identidade de quem solicita informações.
- **Simular ataques:** Realizar testes de *phishing* internos para avaliar a prontidão da equipe.
- **Estabelecer protocolos claros:** Definir processos para validar solicitações sensíveis.

19 Caso Prático: Engenharia Social em Ligação Telefônica

No exemplo citado, o atacante utilizou uma técnica clássica de **pretexting**, onde cria uma história plausível para ganhar a confiança do funcionário. Ações preventivas incluem:

- **Educação contínua:** Ensinar os funcionários a reconhecer e questionar pedidos suspeitos.
- **Verificação de identidade:** Estabelecer procedimentos para autenticar quem faz solicitações de informações sensíveis.
- **Cultura organizacional:** Promover um ambiente onde os colaboradores se sintam à vontade para relatar possíveis ataques.