Tarefa - Segurança da Informação

Arisio Soares Andrade Filho

1. Quais são os desafios mais comuns na implementação de medidas preventivas contra ataques de Denial of Service (DoS) dentro de empresas de médio e grande porte? Como os slides da aula sugere lidar com esses desafios?

Os principais desafios na implementação de medidas preventivas contra ataques de DoS incluem a dificuldade de identificar ataques em tempo real, a necessidade de escalabilidade nas defesas e a complexidade de integrar múltiplas camadas de segurança. Os slides sugerem a utilização de criptografias para aumentar a segurança.

2. Em que medida a gestão de T.I. deve estar envolvida na elaboração e na atualização contínua de políticas de segurança para evitar vulnerabilidades que possam levar a ataques como o DoS?

A gestão de TI deve estar profundamente envolvida na criação, atualização e execução das políticas de segurança. Sendo essencial que a gestão participe ativamente para garantir que as políticas de segurança estejam alinhadas com os objetivos estratégicos da empresa e sejam revisadas regularmente, levando em conta novas ameaças e vulnerabilidades.

3. Como a conscientização dos colaboradores sobre práticas de segurança digital pode reduzir o risco de ataques cibernéticos? Os slides apresentam alguma estratégia para treinamento e conscientização?

A conscientização dos colaboradores sobre segurança digital ajuda a reduzir o risco de ataques cibernéticos porque, quando os funcionários sabem como identificar ameaças como phishing, usar senhas fortes e evitar comportamentos arriscados, eles tornam a organização mais segura. O erro humano é uma das principais causas de ataques, então, quando os colaboradores estão bem treinados, a chance de um ataque acontecer diminui.

4. Qual é o papel das auditorias regulares de segurança na detecção de vulnerabilidades?

As auditorias de segurança são essenciais para identificar vulnerabilidades que podem ser exploradas em ataques cibernéticos, como os DoS. Elas ajudam a verificar se as políticas de segurança estão sendo seguidas corretamente e se as ferramentas de defesa estão funcionando de forma adequada.

5. Em relação ao Denial of Service, quais técnicas podem ser utilizadas para mitigar esse tipo de ataque?

Podemos citar a filtragem de tráfego(utilização de firewalls para identificar e bloquear tráfego malicioso), a Redundância e escalabilidade(Ter servidores e redes redundantes para distribuir o tráfego e garantir que a infraestrutura não fique sobrecarregada) e o Rate Limiting(limita a quantidade de requisições que um servidor pode processar em um determinado período de tempo, dificultando o

ataque.)

6. Cite e explique como funciona os firewalls.

Um firewall é uma ferramenta de segurança que controla o tráfego de rede entre diferentes redes ou dispositivos, com base em um conjunto de regras predefinidas. Ele pode ser configurado para permitir ou bloquear o tráfego de dados dependendo de características como o endereço IP de origem, o destino, o tipo de protocolo, ou até mesmo o conteúdo dos pacotes.

7. Explique os três principios mais importantes se tratando da segurança de dados: Confidencialidade, Integridade e Disponibilidade.

Confidencialidade: Garante que os dados sejam acessados apenas por pessoas ou sistemas autorizados. A confidencialidade é fundamental para evitar que informações sensíveis sejam acessadas ou divulgadas indevidamente.

Integridade: Refere-se à precisão e consistência dos dados. Isso significa garantir que os dados não sejam alterados ou corrompidos, seja de forma acidental ou intencional, e que qualquer alteração seja detectada.

Disponibilidade: Garante que os dados e sistemas estejam acessíveis e funcionais quando necessários. Mesmo diante de falhas ou ataques, as organizações devem garantir que seus sistemas permaneçam operacionais e que os dados possam ser acessados quando necessário.