ATIVIDADE 20 de Agosto - Luana Oliveira Sousa - Gestão de TI. - Robson Calvetti

1. Criptografia em Comunicações Seguras

A criptografia é um dos principais pilares da segurança da informação, e sua aplicação prática está diretamente relacionada à proteção de dados sigilosos contra acessos não autorizados. No caso das comunicações seguras na web, o protocolo *SSL/TLS* é amplamente utilizado. Ele garante que os dados trocados entre um navegador e um servidor sejam criptografados, de modo que mesmo que um atacante intercepte essa comunicação, ele não consiga ler ou alterar as informações sem a chave de decriptação.

- Exemplo Prático: Imagine um usuário acessando seu banco online. Os dados, como senha e número da conta, são enviados criptografados, garantindo que, mesmo que essa comunicação seja interceptada, a pessoa mal-intencionada não consiga acessar as informações.
- Por que é importante?: Proteger a confidencialidade e a integridade dos dados é essencial em operações sensíveis, como transações bancárias e o envio de documentos confidenciais.

2. Controle de Acesso em Sistemas de Informação

O controle de acesso trata da definição de quem pode acessar quais recursos em um sistema e de que maneira. Os sistemas de controle de acesso garantem que apenas pessoas devidamente autenticadas e autorizadas possam interagir com determinados dados ou funcionalidades de um sistema.

- Exemplo Prático: Uma empresa pode implementar o *Autenticação Multifator (MFA)* em seus sistemas de login. Além da senha, os funcionários devem inserir um código gerado em tempo real em seus celulares. Isso dificulta que invasores consigam acessar a conta mesmo que obtenham a senha, já que não têm o segundo fator de autenticação.
- *Por que é importante?*: Sem controles adequados, um atacante que roube credenciais pode acessar informações sensíveis ou realizar ações prejudiciais dentro do sistema, como alterar dados financeiros ou copiar segredos comerciais.

3. Detecção e Prevenção de Intrusões (IDS/IPS)

Os sistemas de detecção de intrusões (*IDS) monitoram o tráfego de rede ou atividades de sistemas em busca de sinais que indiquem ataques ou comportamentos maliciosos, como tentativas de login inválido, acessos não autorizados ou movimentos internos suspeitos dentro da rede. Já os sistemas de prevenção de intrusões (IPS*) são mais ativos, respondendo automaticamente às ameaças, bloqueando ou isolando o tráfego malicioso.

- Exemplo Prático: Uma grande empresa pode instalar um *IDS* em seu datacenter para monitorar o tráfego de entrada e saída. Se um invasor tentar explorar uma vulnerabilidade em um dos sistemas, o IDS poderá alertar os administradores de que há uma tentativa de

ataque, permitindo que eles tomem ações para mitigá-lo. Um *IPS* poderia automaticamente bloquear o ataque assim que detectado.
- Por que é importante?: Esses sistemas são essenciais para identificar ameaças que podem passar despercebidas pelos mecanismos de segurança convencionais, fornecendo uma camada adicional de proteção em tempo real.

4. Segurança de Aplicações Web
Com o crescimento do uso de aplicações web, a segurança dessas aplicações tornou-se um fator crucial para a proteção de dados. Vulnerabilidades como *SQL Injection* e *Cross-Site Scripting (XSS)* são alvos comuns de ataques. Um *SQL Injection* ocorre quando um invasor manipula uma consulta a um banco de dados para roubar ou alterar dados, enquanto o *XSS* permite que atacantes injetem scripts maliciosos em sites legítimos, afetando usuários que visitam a página.

- Exemplo Prático: Um site de e-commerce, para se proteger contra um ataque de *SQL Injection*, implementa parâmetros em suas consultas SQL, em vez de permitir que os usuários insiram livremente códigos maliciosos no campo de pesquisa. Ferramentas automáticas podem ser usadas para testar vulnerabilidades e corrigir falhas.
- *Por que é importante?*: A exploração de vulnerabilidades em aplicações web pode levar ao comprometimento de informações sensíveis de usuários, como dados de pagamento, ou até mesmo à queda total do serviço.

5. Backup e Recuperação de Dados
Backup e recuperação de dados são práticas essenciais para garantir a continuidade dos negócios em caso de falhas catastróficas, ataques cibernéticos, ou desastres naturais. O *backup* é uma cópia dos dados armazenados em um local separado, e a *recuperação* é o processo de restaurar esses dados para garantir que os sistemas voltem a funcionar normalmente após uma falha.

- Exemplo Prático: Uma empresa pode configurar backups automáticos diários de seus dados em servidores de nuvem. Se um ataque de ransomware ocorrer e os arquivos da empresa forem criptografados pelos atacantes, o setor de TI pode restaurar os sistemas a partir dos backups mais recentes, minimizando o impacto do ataque.
- Por que é importante?: A falta de backups adequados pode resultar em perda permanente de dados cruciais para a operação da empresa, além de prejuízos financeiros e danos à reputação.

Esses exemplos destacam como os conceitos de segurança em sistemas computacionais são aplicados de maneira prática para proteger redes, dados e aplicações contra ataques, falhas e acessos não autorizados.