Atividades Professor Calvetti- Davi Emanuel Silva Adriano 823149648

ATIVIDADE LAB1

Resumo sobre Aplicações dos Conteúdos de Sistemas Computacionais

1. Segurança em Dispositivos IoT

A Internet das Coisas (IoT) tem se tornado cada vez mais presente em residências, indústrias e serviços públicos. No entanto, dispositivos IoT apresentam vulnerabilidades de segurança que podem ser exploradas por atacantes. A aplicação de conteúdos de SC nesse contexto envolve a implementação de mecanismos de autenticação robustos, criptografia de comunicação entre dispositivos e monitoramento contínuo para detecção de ameaças. Um exemplo prático é a configuração de firewalls e redes segmentadas para impedir que um dispositivo comprometido afete toda a infraestrutura conectada.

2. Segurança em Aplicativos Bancários

O setor financeiro depende fortemente da segurança computacional para proteger transações eletrônicas e dados sensíveis dos clientes. A aplicação de técnicas de desenvolvimento seguro, como a utilização de autenticação multifator (MFA) e a implementação de protocolos seguros como TLS (Transport Layer Security), ajuda a mitigar riscos de ataques como phishing e engenharia social. Um exemplo é o uso de tokens temporários para confirmação de transações, dificultando a ação de criminosos.

3. Monitoramento e Prevenção de Ataques DDoS

Ataques de negação de serviço distribuídos (DDoS) são uma ameaça comum a serviços online. A detecção e mitigação desses ataques envolvem a aplicação de sistemas de monitoramento de tráfego de rede, uso de redes de distribuição de conteúdo (CDN) para absorver picos de acessos maliciosos e configuração de firewalls específicos para bloqueio automático de endereços IP suspeitos. Empresas de grande porte, como provedores de serviço em nuvem, utilizam sistemas como Cloudflare e AWS Shield para mitigar esses ataques.

4. Forense Computacional para Investigação de Crimes Digitais

A forense computacional é um ramo fundamental da segurança da informação, utilizado para investigar incidentes cibernéticos. Seu uso permite a identificação de responsáveis por ataques, análise de malware e recuperação de dados comprometidos. Ferramentas como Autopsy e FTK Imager são amplamente utilizadas para coleta e análise de evidências digitais. Um caso prático seria a investigação de um ataque ransomware, onde especialistas analisam logs de acesso e registros de rede para determinar a origem do ataque e recuperar arquivos criptografados.

5. Segurança em Sistemas de Comércio Eletrônico

As plataformas de e-commerce necessitam de camadas de segurança para proteger informações dos clientes, como dados de cartões de crédito e histórico de compras. A implementação de protocolos seguros para transmissão de dados, como HTTPS, e o uso de técnicas como *tokenization* para evitar o armazenamento de informações sensíveis são essenciais. Além disso, mecanismos como CAPTCHA e monitoramento de transações suspeitas ajudam a prevenir fraudes. Um exemplo é o uso de sistemas antifraude baseados em aprendizado de máquina, que analisam padrões de compra para identificar possíveis tentativas de fraude.

Os conceitos estudados na UC Sistemas Computacionais têm aplicação em diversas áreas, garantindo a segurança e a eficiência de sistemas digitais. Desde a proteção de redes corporativas até o desenvolvimento seguro de software, cada técnica abordada desempenha um papel fundamental na prevenção e mitigação de riscos cibernéticos. A constante evolução das ameaças digitais torna essencial o aprimoramento contínuo dessas práticas, garantindo um ambiente mais seguro para empresas, governos e usuários finais.