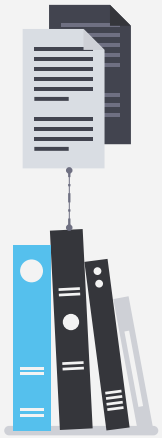
Ataques em Sistemas Distribuídos: Um panorama geral

Análise das principais ameaças e medidas de segurança

Membros do grupo

André Luis Cavalcanti - 01481912
Daniel Lins Aretakis - 01420808
Lucas José Leite Marinho - 01418858
Rafael Hilario Dias Barbosa - 01426126
Wenny Santana de Andrade - 01415774

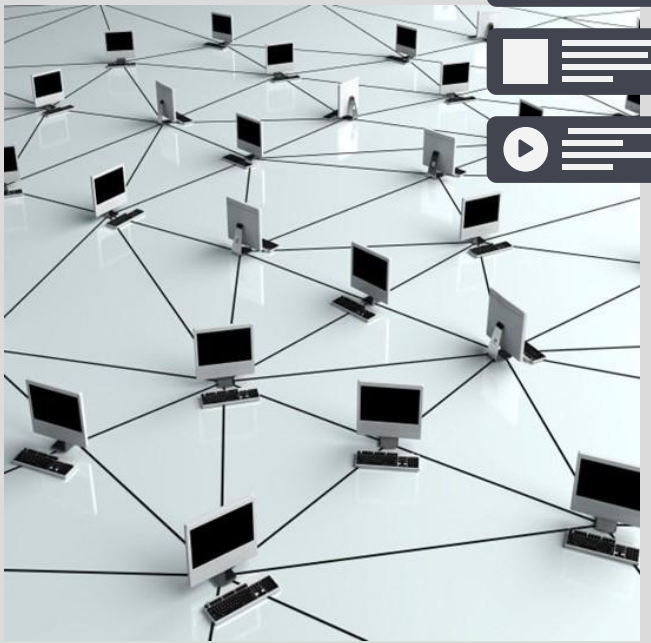


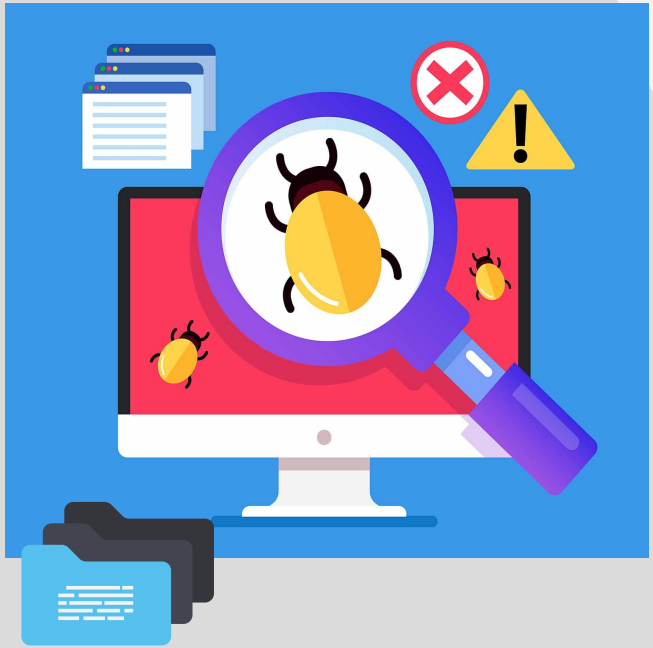
Introdução aos Sistemas Distribuídos

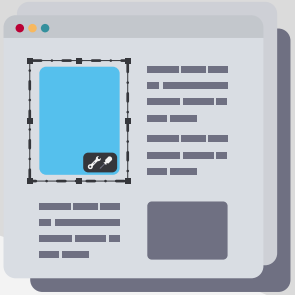
- **Sistemas distribuídos** referem-se a um conjunto de computadores que trabalham de forma colaborativa, conectados por uma rede, visando realizar uma tarefa. Cada máquina no sistema tem uma função específica e compartilha recursos entre si.

- Exemplos cotidianos incluem **sistemas bancários**, **computação em nuvem** e **plataformas de streaming**, amplamente usados no Brasil e em todo o mundo.

- No contexto brasileiro, esses sistemas são críticos para o funcionamento de **serviços financeiros**, **governamentais e de telecomunicações**, que demandam alta disponibilidade e segurança.







01

Vulnerabilidades

Vulnerabilidades em Sistemas Distribuídos

Senhas Fáceis:

Utilização de senhas fracas pode facilitar o acesso não autorizado, comprometendo a segurança dos dados.

Falta de Atualização dos Softwares:

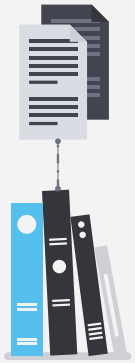
Softwares desatualizados são suscetíveis a vulnerabilidades conhecidas, permitindo exploração por atacantes.

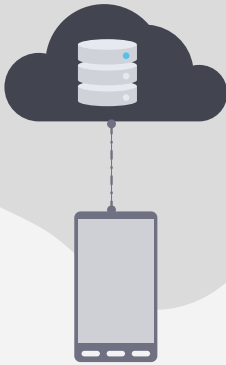
Malware:

Softwares maliciosos podem infectar sistemas distribuídos, prejudicando a integridade e confidencialidade dos dados.

Controle de Credenciais:

Falhas no gerenciamento de credenciais podem permitir acessos indevidos e comprometer a segurança do sistema.





Principais Tipos de Ataques

DoS/DDoS

Ocorrem quando um servidor ou rede é sobrecarregado com solicitações, resultando na interrupção do serviço

Man-in-the-Middle (MITM)

Interceptações durante a comunicação entre dois sistemas. Um invasor pode modificar ou roubar dados enquanto eles estão em trânsito.

Código Móvel:

Ataques a sistemas distribuídos via código móvel usam código malicioso inserido por agentes internos com acesso ao sistema, explorando permissões elevadas.

02

Proteção

Medidas de Prevenção e Mitigação

- **Criptografia de Dados:** Tanto dados em trânsito quanto armazenados devem ser protegidos por criptografia forte, evitando interceptações e acessos não autorizados.

- **Firewalls e IDS/IPS:** Sistemas de firewall e sistemas de detecção/prevenção de intrusões (IDS/IPS) são ferramentas essenciais para monitorar e bloquear acessos maliciosos.

- **Redundância de Sistemas:** Manter réplicas dos sistemas distribuídos pode ajudar a prevenir perdas de dados ou falhas de disponibilidade em caso de ataque.

03

Estudo de caso

Ataque ao Banco Central do Brasil

O ataque:

Em 2020, o Banco Central do Brasil sofreu um ataque de Negação de Serviço Distribuída (DDoS) que interrompeu serviços digitais, como pagamentos online e transferências bancárias.

Impacto:

A interrupção resultou na suspensão de transações financeiras por várias horas, afetando milhões de brasileiros e gerando prejuízos econômicos significativos.

Resposta ao Incidente:

A equipe de TI do Banco Central trabalhou rapidamente para mitigar o ataque, mas enfrentou desafios devido à intensidade do tráfego malicioso.

04

Tendências Futuras

Tendências Futuras e Desafios no Brasil

Uso de Inteligência Artificial

O uso crescente de IA para detecção precoce e mitigação de ataques. Ferramentas automatizadas podem identificar padrões de tráfego anormais e bloquear potenciais ameaças.

Setores Emergentes

A agricultura digital, saúde e infraestrutura crítica no Brasil enfrentam desafios de segurança à medida que digitalizam seus processos, exigindo maior investimento em medidas de cibersegurança.

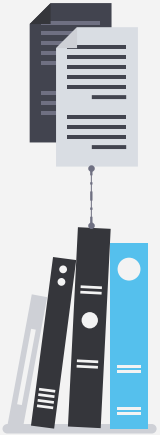
Blockchain para Segurança

A implementação de blockchain em sistemas distribuídos pode fornecer transparência e segurança nas transações, especialmente em setores financeiros e de supply chain.

Desafios

Proteção de infraestruturas críticas, como energia e telecomunicações, é um dos maiores desafios de segurança cibernética no Brasil.

Conclusão



- A segurança cibernética em sistemas distribuídos é essencial para proteger infraestruturas críticas e garantir a continuidade dos serviços.
- Com o aumento da digitalização e da interconectividade, as ameaças estão se tornando mais sofisticadas, exigindo medidas proativas de prevenção e mitigação.
- O futuro da cibersegurança em sistemas distribuídos depende de novas tecnologias, como IA e blockchain, para antecipar e prevenir ataques em tempo real.
- Empresas e governos precisam investir em soluções robustas para evitar que falhas de segurança comprometam dados sensíveis e serviços essenciais.

Obrigado!