Relatório Stride

Prompt Utilizado

Analise cuidadosamente o texto extraído do diagrama de arquitetura e elabore um relatório STRIDE detalhado em português brasileiro. Para cada categoria STRIDE, descreva claramente os riscos, estratégias de mitigação e inclua pelo menos uma referência confiável. Não inclua comentários adicionais ou conclusões após o relatório. Ao final, gere uma tabela em markdown resumindo cada seção STRIDE, seus principais riscos e as respectivas mitigações de forma objetiva.

Texto extraído (em inglês): Develop and end users interact with edge services via blockchain user applications (mobile, wallet, web, CLI) and peer cloud. Edge services connect to the security gateway, provider cloud portal service, and server runtimes within the cloud network. Server runtimes interface with blockchain admin & ops services, which manage membership, consensus, ledger, events, smart contract, and system integration components. API management, transformation & connectivity integrate with enterprise user directory, enterprise applications, and enterprise data in the enterprise network. Information governance, infrastructure security, and security monitoring & intelligence provide underlying support within the cloud network.

Relatório STRIDE

---

1. Spoofing (Falsificação de Identidade)

Riscos:

- Usuários mal-intencionados podem se passar por desenvolvedores, usuários finais ou serviços de edge, obtendo acesso indevido a aplicações blockchain, peer cloud ou serviços na nuvem.
- Ataques de spoofing podem comprometer a autenticação em gateways de segurança, APIs ou diretórios de usuários empresariais.

Mitigações:

- Implementação de autenticação multifator (MFA) para todos os usuários e serviços.
- Uso de certificados digitais e autenticação baseada em identidade para comunicação entre serviços.
- Monitoramento contínuo de tentativas de login e alertas para atividades suspeitas.

Referência:
OWASP Authentication Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

---

2. Tampering (Adulteração)

Riscos:

- Manipulação maliciosa de dados transmitidos entre aplicações blockchain, edge services e cloud services.
- Alteração de contratos inteligentes, eventos do ledger ou dados de integração de sistemas.
- Modificação de APIs expostas, resultando em corrupção de dados empresariais.

Mitigações:

- Uso de criptografia ponta a ponta (TLS/SSL) em todos os canais de comunicação.
- Implementação de assinaturas digitais para garantir a integridade de mensagens e contratos inteligentes.
- Monitoramento de integridade de arquivos e logs para detectar adulterações.

Referência:
NIST SP 800-57 Part 1: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

---

3. Repudiation (Repúdio)

Riscos:

- Usuários ou serviços podem negar a realização de transações ou alterações em contratos inteligentes.

- Falta de trilhas de auditoria pode dificultar a responsabilização por ações realizadas nos sistemas.

Mitigações:

- Implementação de logs imutáveis e trilhas de auditoria detalhadas para todas as operações sensíveis.
- Uso de mecanismos de assinatura digital para garantir não-repúdio em transações blockchain.
- Auditoria regular e validação de logs por equipes independentes.

Referência:
ISO/IEC 27001:2013, seção A.12.4 Logging and monitoring: https://www.iso.org/isoiec-27001-information-security.html

---

4. Information Disclosure (Divulgação de Informação)

Riscos:

- Vazamento de dados sensíveis de usuários, contratos inteligentes, diretórios empresariais ou integrações de dados.
- Exposição indevida de informações através de APIs ou falhas em controles de acesso.

Mitigações:

- Implementação de controles de acesso baseados em papéis (RBAC) e políticas de privilégio mínimo.
- Criptografia de dados em repouso e em trânsito.
- Monitoramento e testes regulares de vulnerabilidades em APIs e serviços.

Referência:
OWASP Top 10 - Sensitive Data Exposure: https://owasp.org/Top10/A03_2021-Sensitive_Data_Exposure/

---

5. Denial of Service (Negação de Serviço)

Riscos:

- Ataques DDoS podem afetar edge services, gateways de segurança, APIs e serviços em nuvem, causando indisponibilidade.
- Sobrecarga de transações ou eventos blockchain pode degradar o desempenho do sistema.

Mitigações:

- Implementação de mecanismos de rate limiting e proteção contra DDoS em todos os pontos de entrada.
- Uso de balanceamento de carga e escalonamento automático de recursos na nuvem.
- Monitoramento proativo de disponibilidade e resposta rápida a incidentes.

Referência:
NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

6. Elevation of Privilege (Elevação de Privilégio)

Riscos:

- Usuários ou serviços podem obter permissões superiores às necessárias, comprometendo a integridade e segurança dos sistemas blockchain e empresariais.
- Exploração de falhas em APIs, gateways ou integrações para acessar funções administrativas.

Mitigações:

- Revisão e restrição rigorosa de permissões de usuários e serviços.
- Implementação de segregação de funções (SoD) e revisões periódicas de privilégios.
- Auditoria de acessos privilegiados e uso de ferramentas de gerenciamento de identidade e acesso (IAM).

Referência:
Microsoft Security Best Practices - Least Privilege: https://docs.microsoft.com/en-us/security/compass/privileged-access-least-privilege

---

Tabela Resumo STRIDE

STRIDE	Principais Riscos	Mitigações Principais
Spoofing	Falsificação de identidade de usuários/serviços	Autenticação multifator, certificados digitais, monitoramento de login
Tampering	Manipulação de dados, contratos inteligentes, APIs	Criptografia ponta a ponta, assinaturas digitais, monitoramento de integridade
Repudiation	Negação de transações/ações, falta de auditoria	Logs imutáveis, assinaturas digitais, auditorias regulares
Information Disclosure	Vazamento de dados sensíveis, exposição via APIs	RBAC, criptografia de dados, testes de vulnerabilidade
Denial of Service	Indisponibilidade por ataques DDoS ou sobrecarga	Rate limiting, proteção DDoS, balanceamento de carga, monitoramento de disponibilidade
Elevation of Privilege	Obtenção indevida de permissões administrativas	Restrição de permissões, segregação de funções, auditoria de acessos, IAM