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): The diagram shows users (Develop User, End User, Blockchain User) interacting with Blockchain User Application through various interfaces (Mobile, Wallet, Web, CLI), connecting to Edge Services in the Cloud Network. Edge Services interact with Security Gateway, Provider Cloud Portal Service, Server Runtimes, and Transformation & Connectivity. Peer Cloud connects to Blockchain Admin & Ops Services, which includes Membership, Consensus, Ledger, Events, Smart Contract, and System Integration. Server Runtimes interface with API Management and Transformation & Connectivity, which connects to the Enterprise Network, including Enterprise User Directory, Enterprise Applications, and Enterprise Data. Information Governance, Infrastructure Security, and Security Monitoring & Intelligence provide overarching governance, security, and monitoring.

Relatório STRIDE

---

1. Spoofing (Falsificação de Identidade)

Riscos:

- Usuários mal-intencionados podem se passar por usuários legítimos (Develop User, End User, Blockchain User) para acessar o Blockchain User Application.
- Possibilidade de falsificação de identidades nos acessos via interfaces (Mobile, Wallet, Web, CLI).
- Ataques de spoofing entre Edge Services e Security Gateway, comprometendo a autenticação de serviços.

Mitigações:

- Implementação de autenticação multifator (MFA) para todos os tipos de usuários e interfaces.
- Uso de certificados digitais e autenticação baseada em identidade para comunicações entre serviços.
- Integração com Enterprise User Directory para centralizar e fortalecer a gestão de identidades.

Referência:
NIST SP 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management
https://pages.nist.gov/800-63-3/sp800-63b.html

---

2. Tampering (Violação de Integridade)

Riscos:

- Manipulação de dados trafegados entre usuários, aplicações e serviços (por exemplo, alteração de transações blockchain ou comandos via CLI).
- Alteração não autorizada de smart contracts, eventos ou dados no Ledger.
- Modificação de APIs expostas pelo API Management.

Mitigações:

- Uso de criptografia ponta a ponta (TLS/SSL) para todas as comunicações.
- Implementação de controles de integridade e assinatura digital para smart contracts e transações.
- Monitoramento contínuo e auditoria de logs de alteração em componentes críticos.

Referência:
OWASP Application Security Verification Standard (ASVS) – Section 8: Data Protection
https://owasp.org/www-project-application-security-verification-standard/

---

3. Repudiation (Repúdio)

Riscos:

- Usuários ou serviços negando a autoria de ações realizadas, como submissão de transações ou modificações em contratos inteligentes.
- Falta de rastreabilidade nas interações entre Edge Services, Provider Cloud Portal Service e Blockchain Admin & Ops Services.

Mitigações:

- Implementação de logs imutáveis e detalhados para todas as operações sensíveis.
- Uso de mecanismos de assinatura digital para garantir a autoria das transações.
- Integração de sistemas de auditoria com Information Governance para garantir conformidade.

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

---

4. Information Disclosure (Divulgação Indevida de Informação)

Riscos:

- Vazamento de dados sensíveis dos usuários via interfaces (Mobile, Wallet, Web, CLI) ou durante a transmissão entre serviços na nuvem.
- Exposição de informações confidenciais do Enterprise User Directory, Enterprise Applications ou Enterprise Data.
- Falhas em Security Gateway ou API Management permitindo acesso não autorizado a dados.

Mitigações:

- Criptografia de dados em repouso e em trânsito.
- Controle de acesso baseado em privilégios mínimos (least privilege) e segregação de funções.
- Monitoramento e alertas de acessos não autorizados implementados por Security Monitoring & Intelligence.

Referência:
GDPR – Art. 32: Security of processing
https://gdpr-info.eu/art-32-gdpr/

---

5. Denial of Service (Negação de Serviço)

Riscos:

- Ataques de negação de serviço direcionados às interfaces de usuário (Mobile, Web, CLI), Edge Services ou Security Gateway, tornando o sistema indisponível.
- Sobrecarga intencional de API Management ou Transformation & Connectivity, afetando a integração com Enterprise Network.

Mitigações:

- Implementação de mecanismos de rate limiting e proteção contra DDoS em todos os pontos de entrada.

- Redundância e escalabilidade automática (auto-scaling) nos serviços críticos.
- Monitoramento proativo de disponibilidade e resposta a incidentes.

Referência:
OWASP Cheat Sheet Series – Denial of Service
https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html

---

6. Elevation of Privilege (Elevação de Privilégio)

Riscos:

- Usuários comuns obtendo privilégios administrativos no Blockchain Admin & Ops Services ou Server Runtimes.
- Exploração de vulnerabilidades em Transformation & Connectivity para acessar Enterprise Applications ou Enterprise Data com privilégios elevados.

Mitigações:

- Implementação de controles rigorosos de gestão de privilégios e revisão periódica de permissões.
- Uso de autenticação forte e segregação de funções administrativas.
- Monitoramento contínuo de tentativas de acesso privilegiado e resposta automática a incidentes.

Referência:
NIST SP 800-53 Rev. 5 – AC-6 Least Privilege
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

---

Tabela Resumo STRIDE

STRIDE	Principais Riscos	Mitigações Principais
Spoofing	Falsificação de identidade de usuários e serviços	MFA, certificados digitais, integração com diretório corporativo
Tampering	Manipulação de dados, contratos e APIs	Criptografia ponta a ponta, assinaturas digitais, auditoria
Repudiation	Negação de autoria de ações e transações	Logs imutáveis, assinaturas digitais, auditoria integrada
Information Disclosure	Vazamento de dados sensíveis e acesso não autorizado	Criptografia, controle de acesso, monitoramento
Denial of Service	Indisponibilidade de serviços por ataques ou sobrecarga	Rate limiting, proteção DDoS, escalabilidade e monitoramento
Elevation of Privilege	Usuários comuns obtendo privilégios administrativos	Gestão de privilégios, segregação de funções, autenticação forte, monitoramento de acessos privilegiados