Arquitetura de Segurança Datanomik

Sumário

1. Resumo Executivo 3
2. Gestão de Credenciais e Segredos 3
3. Segurança da Infraestrutura 4
4. Criptografia de Dados 4
5. Desenvolvimento Seguro e Testes Ofensivos 4
6. Conformidade e Privacidade (LGPD) 5

1. Resumo Executivo

A segurança é o pilar fundamental da operação da Datanomik. Como uma plataforma que processa dados financeiros críticos, adotamos uma postura de "Security First", implementando controles de nível bancário em todas as camadas da nossa arquitetura. Este documento detalha como garantimos a confidencialidade, integridade e disponibilidade dos dados de nossos clientes.

2. Gestão de Credenciais e Segredos

Compreendemos que o compartilhamento de credenciais bancárias é o ponto mais sensível da operação. Para mitigar o risco de exposição, utilizamos uma arquitetura de Cofre Digital:

- **Isolamento de Credenciais:** As senhas e chaves de API inseridas na plataforma Datanomik nunca são armazenadas em texto plano.
- **Criptografia Assimétrica:** No momento da inserção, a credencial é imediatamente criptografada utilizando algoritmos fortes (AES-256) e armazenada em um serviço de gerenciamento de segredos (AWS Secrets Manager).
- **Acesso Máquina-a-Máquina:** Apenas os microsserviços de automação (APIs) possuem permissão programática para descriptografar as credenciais temporariamente em memória volátil para executar a transação. Nenhum colaborador humano (desenvolvedores ou suporte) possui acesso às chaves de descriptografia.
- **Rotação de Chaves:** As chaves de criptografia são rotacionadas periodicamente, garantindo que, mesmo em um cenário hipotético de vazamento de banco de dados, as informações permaneceriam ilegíveis.

3. Segurança da Infraestrutura

Nossa infraestrutura é hospedada em um provedor de nuvem de classe mundial AWS Cloud, certificada na ISO 27001, SOC 2.

- **Segregação de Ambientes:** Mantemos ambientes estritamente segregados para Desenvolvimento, Homologação e Produção. Dados reais de clientes residem apenas em Produção e nunca são utilizados para testes.
- **Rede Privada Virtual:** Nossos servidores e bancos de dados não são expostos diretamente à internet pública. O acesso é restrito via VPN com autenticação forte e limitado a endereços IP autorizados.
- **Proteção contra DDoS:** Utilizamos camadas de proteção (WAF) para mitigar ataques de negação de serviço e filtrar tráfego malicioso antes que ele atinja nossa aplicação.

4. Criptografia de Dados

Implementamos criptografia em todo o ciclo de vida do dado:

- **Dados em Trânsito:** Toda comunicação entre o cliente e a Datanomik, bem como entre a Datanomik e as Instituições Financeiras, é criptografada via TLS 1.2 ou superior.
- **Dados em Repouso:** Todos os bancos de dados, volumes de armazenamento e backups são criptografados utilizando o padrão AES-256.

5. Desenvolvimento Seguro e Testes Ofensivos

Nossa metodologia de desenvolvimento segue as diretrizes da OWASP:

- **Pentests Recorrentes:** Submetemos nossa infraestrutura a Testes de Intrusão periódicos, realizados por consultorias independentes, para identificar e corrigir vulnerabilidades.
- **Code Review:** Todo código passa por revisão por pares e análise estática de segurança antes de ser aprovado para produção.

6. Conformidade e Privacidade (LGPD)

A Datanomik atua em conformidade com a Lei Geral de Proteção de Dados (Lei 13.709/2018):

- **Papel de Operador:** Atuamos estritamente como Operadores dos dados, seguindo as instruções configuradas pelo Controlador.
- **Minimização de Dados:** Coletamos apenas os dados estritamente necessários para a execução das transações financeiras e conciliação.
- **Programa de Governança:** Estamos em processo de implementação da ISO/IEC 27001, a norma internacional de referência para Gestão de Segurança da Informação.

Datanomik Security Team Em caso de dúvidas, entre em contato: cyber@datanomik.com