FUNDAÇÃO ESCOLA DE COMÉRCIO ÁLVARES PENTEADO
FECAP

CENTRO UNIVERSITÁRIO ÁLVARES PENTEADO

Análise e Desenvolvimento de Sistemas

Ana Clara Torres Musso
Arthur Felipe Alves Nunes
Déborah Pavanelli Colicchio
Raissa Elias Silva

Análise de Riscos, vulnerabilidades e ameaças

São Paulo

ANO

Ana Clara Torres Musso
Arthur Felipe Alves Nunes
Déborah Pavanelli Colicchio
Raissa Elias Silva

ANÁLISE DE RISCOS, VULNERABILIDADES E AMEAÇAS

Projeto Integrador do curso apresentado à Fundação Escola de Comércio Álvares Penteado - FECAP, como parte dos requisitos para a obtenção do título de tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Prof. Ronaldo Araújo Pinto

São Paulo

Ano

Resumo

A análise realizada foi dividida em três dimensões principais; risco:estão relacionados a falhas de disponibilidade da API, mudanças em seu formato, baixa usabilidade da interface e desempenho insuficiente ao lidar com grandes volumes de dados. A dependência direta da Cannoli também foi identificada como um risco de alto impacto; ameaças:destacam-se ataques cibernéticos, uso indevido de credenciais, encerramento da API e riscos competitivos. Esses fatores, em grande parte externos, podem comprometer tanto a segurança quanto a relevância do sistema; e vulnerabilidades: foram identificadas fragilidades internas do projeto, como armazenamento inseguro de credenciais, falta de autenticação robusta, ausência de logs e monitoramento, e dependência excessiva da conectividade de rede sem mecanismos de cache.

Palavras-chave: Análise; Risco; Ameaças; Vulnerabilidade;

Abstract

The analysis was divided into three main dimensions: risks – related to API availability failures, format changes, low interface usability, and insufficient performance when handling large volumes of data. The direct dependency on Cannoli was also identified as a high-impact risk; threats – including cyberattacks, misuse of credentials, API discontinuation, and competitive risks. These factors, largely external, can compromise both the security and the relevance of the system; and vulnerabilities – internal weaknesses of the project were identified, such as insecure credential storage, lack of robust authentication, absence of logging and monitoring, and excessive reliance on network connectivity without caching mechanisms.

Key-words: Analysis; Risks; Threats; Vulnerabilities.

1 Introdução

O presente trabalho tem como objetivo realizar um levantamento e análise de riscos, vulnerabilidades e ameaças associados ao projeto de desenvolvimento de uma interface gráfica para exibição de relatórios obtidos por meio da API da empresa Cannoli.

A Cannoli é uma foodtech especializada em apoiar restaurantes e lanchonetes no aumento de suas vendas por meio da análise de dados de consumo. A solução proposta, ao consumir a API da empresa, deve garantir segurança, estabilidade e eficiência para manter a confiabilidade do sistema e a adesão dos usuários finais.

A gestão de riscos em segurança da informação torna-se essencial nesse contexto, permitindo prevenir, mitigar e responder a incidentes, garantindo a continuidade do projeto e a proteção dos dados tratados.

2 Conceitos Fundamentais

2.1. Risco: é a probabilidade de que uma ameaça explore uma vulnerabilidade, causando impacto negativo à organização. De acordo com a ABNT NBR ISO 31000, risco é o “efeito da incerteza nos objetivos”, podendo ser positivo ou negativo.

2.1.1. Ameaça: potencial causa de um incidente indesejado, que pode resultar em prejuízo ao sistema ou à organização (Hintzbergen, Smulders, Baars).

2.1.1.1. Vulnerabilidade: fraqueza ou ausência de proteção em um ativo que pode ser explorada por uma ameaça.

2.1.1.1.1. Exposição: circunstância de estar suscetível a perdas provenientes de um agente ameaçador.

2.1.1.1.1.1. Tipos de riscos: financeiros; operacionais; legais e regulatórios; reputação; estratégicos; de conformidade; segurança da informação

3 Fontes de requisitos de Segurança da Informação

3.1. Análise de riscos: como os identificados no projeto (API fora do ar, dependência de terceiros).

3.1.1. Legislação e regulamentações: incluindo a LGPD e contratos firmados com a Cannoli.

3.1.1.1. Requisitos de negócio: garantir disponibilidade contínua, relatórios confiáveis e boa experiência de uso.

4 Atividades de avaliação de risco

4.1. Caracterização do sistema: identificar componentes (API, GUI, rede, banco de dados, usuários).

4.1.1. Identificação de ameaças: ataques cibernéticos, uso indevido de credenciais, falha de suporte.

4.1.1.1. Identificação de vulnerabilidades: armazenamento inseguro, ausência de logs, dependência da rede.

4.1.1.1.1. Análise de controles existentes: autenticação básica já implementada, mas sem monitoramento contínuo.

4.1.1.1.1.1. Determinar probabilidade da ocorrência: riscos técnicos (médio a alto), riscos de desastre natural (baixo).

4.1.1.1.1.1.1. Análise de impacto: alto impacto em caso de indisponibilidade da API ou vazamento de dados.

4.1.1.1.1.1.1.1.Determinação do risco: combinação probabilidade × impacto (ex.: API instável → risco alto).

4.1.1.1.1.1.1.1. Recomendações de controle: autenticação forte, monitoramento de logs, cache local.

4.1.1.1.1.1.1.1. Documentação da avaliação: este relatório constitui o registro formal da análise.

5 Análises de risco do projeto

5.1. Riscos:

- API fora do ar ou instável.
- Mudanças em endpoints ou formato de dados.
- Baixa usabilidade da interface gráfica.
- Desempenho insuficiente com grandes volumes de dados.
- Dependência de terceiros (Cannoli).

5.1.1. Vulnerabilidades:

- Armazenamento inseguro de credenciais.
- Falta de autenticação e controle de acesso robustos.
- Ausência de logs e monitoramento.
- Dependência da conectividade sem mecanismos de cache.
- Testes insuficientes em versões finais.

5.1.1.1. Ameaças:

- Ataques cibernéticos (roubo de dados, DDoS).

- Uso indevido de credenciais (vazamento de chaves de API).
- Perda de suporte da Cannoli.
- Riscos competitivos (entrada de soluções similares).

6 Métodos de avaliação e priorização

6.1. Análise Qualitativa: classificação dos riscos como Baixo, Médio ou Alto.

6.1.1. Análise Quantitativa: atribuir valores quando possível (ex.: perda financeira estimada em caso de indisponibilidade).

6.1.1.1. Matriz GUT (Gravidade, Urgência, Tendência): priorizar riscos mais críticos.

6.1.1.1.1. Mapa de calor: visualização de riscos conforme probabilidade e impacto.

7 NIST Security Framework

7.1. Identificar (ID): inventário de ativos (API, GUI, dados de vendas).

7.1.1. Proteger (PR): autenticação forte, criptografia, cache local.

7.1.1.1. Detectar (DE): monitoramento de acessos e falhas de rede.

7.1.1.1.1. Responder (RS): plano de resposta em caso de indisponibilidade da API.

7.1.1.1.1.1. Recuperar (RC): restauração via backups e fallback de dados.

8 Contramedidas e estratégias de mitigação

8.1. Prevenção: firewall, políticas de senha, criptografia.

8.1.1. Detecção: monitoramento de logs, alertas de anomalias.

8.1.1.1. Repressão: backup automático dos relatórios.

8.1.1.1.1. Correção: aplicação de patches e atualizações de software.

8.1.1.1.1.1. Seguro: proteção contra perdas financeiras.

8.1.1.1.1.1.1. Aceitação: em riscos de baixo impacto ou custo de mitigação elevado.

8.1.1.1.1.1.1.1. Lições aprendidas: registro de falhas anteriores (ex.: semestre passado com perda de suporte).

9 Tipos de ameaças e danos

9.1. Humanas intencionais: ataques internos ou externos maliciosos.

9.1.1. Humanas não intencionais: exclusão acidental de dados, má configuração.

9.1.1.1. Não humanas: queda de energia, falhas de rede, eventos climáticos.

9.1.1.1.1. Danos diretos: vazamento de dados de vendas, roubo de credenciais.

9.1.1.1.1.1. Danos indiretos: perda de clientes por indisponibilidade da API, danos à reputação.

10 Conclusão

A análise evidencia que o sucesso do projeto depende diretamente da capacidade de antecipar problemas e implementar medidas de mitigação eficazes.

A aplicação das metodologias apresentadas (NIST SP 800-30, NIST CSF, matriz GUT) possibilita não apenas a prevenção de incidentes, mas também a resposta rápida e a recuperação eficiente em situações adversas.

Assim, a gestão de riscos deve ser entendida como um processo contínuo, garantindo confiabilidade, escalabilidade e valor agregado ao negócio da Cannoli e de seus parceiros.