Centro Universitário - Fundação Escola de Comércio Álvares Penteado (FECAP)
Curso: Análise e Desenvolvimento de Sistemas

Título: Levantamento de Riscos, Vulnerabilidades e Ameaças em Cibersegurança

Aluno: Vinícius Brandão, Murilo Dias, Guilherme Rodrigues e João Henrique Albuquerque
Professor: Ronaldo Araujo
Disciplina: Cibersegurança e Defesa Cibernética

São Paulo
2025

Sumário

---

1. Introdução

Este documento unifica informações relacionadas ao projeto **Sistema de Gestão de *Fast And Cheap*** e conceitos avançados de cibersegurança. O foco é identificar e analisar riscos, vulnerabilidades e ameaças em projetos tecnológicos que envolvem coleta e processamento de dados em plataformas web e aplicativos móveis.

---

2. Riscos em Cibersegurança

2.1 Violação de Dados (Data Breach)

- **Descrição:** Acesso não autorizado a informações sensíveis dos usuários.
- **Impactos:** Perda de confiança, sanções legais e financeiras.

2.2 Ataques DDoS

- **Descrição:** Sobrecarga de servidores, tornando o serviço indisponível.
- **Impactos:** Interrupção do serviço e prejuízos financeiros.

2.3 Acesso Não Autorizado

- **Descrição:** Invasores obtêm acesso a sistemas críticos.
- **Impactos:** Comprometimento da integridade do sistema.

2.4 Ataques de Engenharia Social (Phishing)

- **Descrição:** Induz usuários a revelar credenciais ou informações sensíveis.
- **Impactos:** Perda de dados e acesso indevido.

2.5 Exploração de APIs Inseguras

- **Descrição:** Uso de APIs sem proteções adequadas.
- **Impactos:** Exposição de dados e manipulação indevida.

2.6 Riscos Legais e Regulatórios

- **Descrição:** Descumprimento de leis e normas de proteção de dados.
- **Impactos:** Multas e danos à reputação.

2.7 Concorrência Acirrada e Baixa Adoção

- **Descrição:** Concorrência intensa e falta de aceitação do mercado.
- **Impactos:** Redução de usuários e retorno financeiro.

---

3. Vulnerabilidades Comuns

- **Autenticação Fraca:** Senhas simples e ausência de MFA.
- **Softwares Desatualizados:** Facilitação de ataques conhecidos.
- **APIs Mal Configuradas:** Falta de autenticação robusta.
- **Criptografia Inadequada:** Dados sem proteção robusta.
- **Gestão de Sessão Deficiente:** Sessões sem expiração adequada.
- **Infraestrutura Insuficiente:** Capacidade limitada para suportar picos de acesso.

---

4. Ameaças Relevantes

- **Malware e Ransomware:** Sequestro e criptografia de dados.
- **Injeção de SQL (SQLi):** Manipulação de bancos de dados.
- **Cross-Site Scripting (XSS):** Scripts maliciosos em aplicações web.
- **Man-in-the-Middle (MitM):** Interceptação de dados.
- **Ataques de Força Bruta:** Tentativas automatizadas para descoberta de senhas.
- **Ameaças Humanas e Naturais:** De funcionários insatisfeitos a desastres naturais.

---

5. Medidas de Mitigação

- **Autenticação Multifator (MFA):** Reduz o risco de acesso não autorizado.
- **Criptografia Robusta:** TLS para transmissão e AES-256 para armazenamento.
- **Monitoramento Contínuo:** Logs para detectar comportamentos suspeitos.
- **Testes de Penetração (Pentests):** Identificação e correção de falhas.
- **Política de Atualizações:** Correções regulares de software.
- **Hardening de APIs:** Limites de taxa e validação rigorosa.
- **Educação e Treinamento:** Conscientização sobre ameaças sociais.
- **Planos de Resposta e Recuperação:** Procedimentos para restaurar o serviço.

---

6. Metodologias Aplicadas

- **NIST Cybersecurity Framework:** Identificar, Proteger, Detectar, Responder e Recuperar.
- **Matriz GUT (Gravidade, Urgência e Tendência):** Priorização de riscos.
- **Análise SWOT:** Avaliação de forças, fraquezas, oportunidades e ameaças.
- **ABNT NBR ISO/IEC 27002:** Estabelecimento de requisitos de segurança.

---

7. Conclusão

A adoção de práticas robustas de cibersegurança é essencial desde o início do projeto **Sistema de Gestão de *Fast And Cheap***. Medidas preventivas, associadas a monitoramento contínuo, garantem resiliência organizacional, proteção de dados sensíveis e confiança dos usuários.