OrganizAi NIST

Introdução

Este documento descreve a implementação do NIST Cybersecurity Framework (CSF) para o aplicativo OrganizAi, um aplicativo financeiro pessoal projetado para ajudar os usuários a gerenciar suas finanças, descobrir benefícios governamentais e comparar preços de aplicativos de viagens. O aplicativo lida com dados financeiros confidenciais e informações pessoais identificáveis (PII), tornando a segurança cibernética uma prioridade máxima. Este documento estabelece as diretrizes e controles de segurança para proteger os dados dos usuários e garantir a integridade do aplicativo.

Objetivo

O objetivo deste documento é:

- Fornecer uma estrutura para a gestão de riscos de segurança cibernética do aplicativo OrganizAi, alinhada com o NIST CSF.
- Identificar e proteger os ativos de informação do aplicativo, incluindo dados financeiros, PII e infraestrutura de TI.
- Estabelecer controles de segurança para prevenir, detectar e responder a incidentes de segurança cibernética.
- Garantir a conformidade com as regulamentações de proteção de dados, como a LGPD.
- Promover uma cultura de segurança cibernética em toda a organização.
- Garantir a confidencialidade, integridade e disponibilidade dos dados do usuário.
- Demonstrar o compromisso da organização com a segurança cibernética e a proteção dos dados do usuário.

1. Identificar (Identify):

1.1. **Ativos:**

1.1.1. Dados financeiros dos usuários (receitas, despesas, benefícios, histórico de viagens).
1.1.2. Informações pessoais identificáveis (PII).
1.1.3. Códigos-fonte do aplicativo.
1.1.4. Servidores e bancos de dados.
1.1.5. Chaves de criptografia.

1.2. **Riscos:**

1.2.1. Acesso não autorizado aos dados financeiros.
1.2.2. Roubo de PII.
1.2.3. Vulnerabilidades no código do aplicativo.
1.2.4. Perda de dados devido a falhas de servidor.
1.2.5. Ataques de phishing para roubar credenciais.

1.3. **Controles:**

1.3.1. Inventário de todos os ativos de hardware e software.
1.3.2. Classificação dos dados com base na sensibilidade.
1.3.3. Avaliação de risco para identificar vulnerabilidades.

2. Proteger (Protect):

2.1. **Controles de acesso:**

2.1.1. Autenticação multifator (MFA).
2.1.2. Controles de acesso baseados em função.
2.1.3. Políticas de senhas fortes.

2.2. **Proteção de dados:**

2.2.1. Criptografia de dados em trânsito e em repouso.
2.2.2. Mascaramento de dados sensíveis.
2.2.3. Backups regulares de dados.

2.3. **Segurança de aplicativos:**

2.3.1. Testes de segurança de aplicativos (SAST, DAST).
2.3.2. Desenvolvimento seguro de software (SDLC).
2.3.3. Atualizações de segurança regulares.

2.4. **Conscientização e treinamento:**

2.4.1. Treinamento de segurança cibernética para desenvolvedores e funcionários.
2.4.2. Conscientização do usuário sobre phishing e outras ameaças.

3. Detectar (Detect):

3.1. **Monitoramento contínuo:**

3.1.1. Sistemas de detecção de intrusão (IDS).
3.1.2. Monitoramento de logs de segurança.
3.1.3. Análise de comportamento do usuário.

3.2. **Detecção de anomalias:**

3.2.1. Alertas para atividades incomuns.
3.2.2. Detecção de fraude.

3.3. **Gerenciamento de eventos de segurança:**

3.3.1. Coleta e análise de logs de segurança.
3.3.2. Correlação de eventos de segurança.

4. Responder (Respond):

4.1. **Planejamento de resposta a incidentes:**

4.1.1. Desenvolvimento de um plano de resposta a incidentes.
4.1.2. Definição de funções e responsabilidades.
4.1.3. Testes regulares do plano de resposta a incidentes.

4.2. **Comunicação:**

4.2.1. Notificação de violações de dados aos usuários afetados.
4.2.2. Comunicação com autoridades reguladoras.

4.3. **Análise pós-incidente:**

4.3.1. Análise da causa raiz dos incidentes.
4.3.2. Implementação de medidas corretivas.

5. Recuperar (Recover):

5.1. **Plano de recuperação de desastres:**

5.1.1. Desenvolvimento de um plano de recuperação de desastres.
5.1.2. Backups de dados e sistemas.
5.1.3. Testes regulares do plano de recuperação de desastres.

5.2. **Comunicação:**

5.2.1. Comunicação com os usuários sobre o status da recuperação.
5.2.2. Restauração de sistemas e dados.

5.3. **Melhorias:**

5.3.1. Implementar melhorias com base nas lições aprendidas com os incidentes.