Centro universitário Fecap- Fundação Escola de Comércio Álvares Penteado

Disciplina: Cibersegurança e Defesa Cibernética

Assunto: NIST Cybersecurity Framework

Integrantes: Isaac Ferreira RA:23025417, Icaro Luiz RA:23025413, Giovanne Braga RA:23025648, Carol Gomes RA:23024619

1. Identificar (Identify - ID)

Ativos Sensíveis:

- Banco de dados (armazenamento de usuários, histórico de preços).
- APIs externas (conexão com Uber, 99, InDrive).
- Back-end na nuvem (Processamento de requisições e armazenamento de dados, código fonte do modelo de IA).
- Aplicativo móvel (Aplicativo mobile e possíveis painéis administrativos).

Principais Ameaças:

- Vazamento de dados e informações do usuário.
- Utilização inadequada de APIs externas.
- Injeção SQL e ataques XSS.
- DDoS contra back-end.
- Uma infraestrutura mal configurada, podendo causar um vazamento de informações.
- Funcionários que não estejam satisfeitos.
- Tratamentos errados em erros de seções, trazendo dados senciveis.

2. Proteger (Protect - PR)

Medidas de Segurança:

Criptografia: Usar AES para armazenar dados confidenciais e TLS para comunicação.

Controle de Acesso: Autenticação via OAuth 2.0/JWT e funcionalidades básicas dentro dos recursos.

Sanitização de Entrada: evitar injeção de SQL e XSS em seu código.

Política de Atualização: Manutenção periódica e revisão de bibliotecas usadas e framework.

Treinamento de funcionários: treinamento para funcionários é bonificações pelo trabalho.

3. Detectar (Detect - DE)

Estratégias de Detecção:

Logging: Para que possa rastrear e ter um, registro de acessos e requisições suspeitas.

Análise de Padrões: gerar alertas para detectar anomalias no uso de requisições

Monitoramento Contínuo: Usar ferramentas SIEM para identificar e detectar ameaças.

4. Resposder (Respond - RS)

Plano de Ação em Caso de Ataque:

Bloqueio Automático: suspender tokens suspeitos.
Notificação aos usuários: Notificar os usuários quando ocorrer uma violação de dados.
Definição de plano: Identificar a origem do ataque e tomar as ações de mitigação necessárias para resolver o problema.

5. Recuperar (Recover - RC)

Medidas Pós-Ataque:

Backups Regulares: implementar backups regulares, para a restauração rápida dos dados.
Revisão de Segurança: Identificar falhas anteriores, e melhorar a segurança para futuros possíveis ataques.
Planos de Continuidade: para garantir a rápida recuperação do serviço após um ataque.