Implementação de Práticas de Segurança da Informação - **Empresa BetaSoft**

João dos Santos Neto
Jamile Jovita da Silva
Ueslei Ferreira dos Reis Ribeiro
Luís Clício Carvalho Sá

Sumário

1. Contexto da Empresa

BetaSoft: Empresa especializada no setor de tecnologia, que desenvolve plataformas digitais de e-commerce para pequenas e médias empresas.

2. Problema

- Injeção SQL comprometeu o banco de dados de uma das suas plataformas de e-commerce.
- Exploração de falhas na interação entre sistemas WEB e um Banco de Dados.
- Permitiu que atacantes explorassem vulnerabilidades no sistema, obtendo acesso não autorizado a informações sensíveis dos clientes.

3. Solução com Segurança da Informação

- Abordagem abrangente
- Auditoria minuciosa
- Incorporação da ISO 27001
- Fortalecimento das defesas com padrão internacional
- Alicerce sólido
- Alinhamento com princípios da ISO 27001
- Base para melhoria contínua

4. Análise de Risco

- **Foco na Injeção SQL:** concentração em uma ameaça crítica.
- **Identificação de ativos em risco:** dados dos clientes e informações estratégicas da empresa.
- **Vulnerabilidades identificadas:** falta de atualizações de software e revisões nas validações nos campos de entrada.
- **Porta de entrada para ataques:** as vulnerabilidades encontradas são vetores para ataques de injeção SQL.

4. Análise de Risco

Principais Características e Riscos de Injeção SQL:

- **Entrada não validada:** aceita dados do usuário sem validação.
- **Concatenação de strings SQL:** inserção de instruções maliciosas.
- **Escopo da injeção:** afeta consultas SELECT, INSERT, UPDATE, DELETE.
- Impactos Potenciais:
    - **Acesso não autorizado e vazamentos:** exposição de dados sensíveis dos usuários e impacto na reputação da organização.
    - **Modificação ou exclusão de registros:** comprometimento da integridade dos dados.
    - **Execução de comandos adicionais:** ameaça à funcionalidade do sistema.

5. Implementação de Controles de Segurança

- Uso de declarações preparadas (com parâmetros)
- Escape de caracteres especiais
- Validação de entrada
- Monitoramento e Registro

6. Criação de Política de Segurança da Informação

- Análise Pós-Incidente
- Atualização da Política de Segurança da Informação
- Treinamento e Conscientização
- Gestão de Crises

7. Auditoria e Plano de Contingência

- **Resposta estratégica:** medidas abrangentes para fortalecer os controles de segurança em toda a infraestrutura.
- **Auditoria abrangente:** identificação não apenas vulnerabilidades relacionadas à injeção SQL, mas também pontos de potencial exposição.
- **Abordagem proativa:** análise completa da postura de segurança para a implementação de medidas preventivas e corretivas.
- **Atualizações software:** atualizações regulares de software emergiram como prática crucial.
- **Importância da atualização constante:** reconhecimento da importância de manter todos os sistemas, frameworks e bibliotecas atualizados para mitigar vulnerabilidades conhecidas.
- **Contribuição para resiliência:** postura de segurança resiliente diante das ameaças em constante evolução no cenário cibernético.

8. Conclusão

A **BetaSoft** enfrentou os desafios da **injeção SQL**, incorporando práticas preventivas em sua política de segurança da informação. A constante atualização dos controles de segurança demonstra a maturidade da empresa em lidar com ameaças emergentes. Agora está mais resiliente na proteção dos dados dos clientes, reconstrução da confiança e fortalecimento de sua posição no mercado.

Dúvidas?