Ministério da Educação
Universidade Federal do Piauí – UFPI
Campus Senador Helvídio Nunes de Barros – Picos
Bacharelado Em Sistemas de Informação
Auditoria e Segurança de Sistemas de Informação
Prof. Júlio Vítor Monteiro Marques

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

Implementação de Práticas de Segurança da Informação na Empresa Fictícia BetaSoft

Picos–PI, 2024

1. Contexto da Empresa

A BetaSoft é uma renomada empresa especializada no desenvolvimento de plataformas digitais de e-commerce, direcionadas principalmente para pequenas e médias empresas. Sua abordagem personalizada e focada nas necessidades específicas dos clientes destaca-se no setor, onde a inovação e a qualidade são imperativas. Com uma missão clara de facilitar e impulsionar as vendas online, a BetaSoft destaca-se pelo design, programação, integração, hospedagem e suporte técnico oferecidos em suas soluções completas de lojas virtuais.

Ao longo dos anos, a BetaSoft construiu uma sólida reputação como parceira confiável para empresas que buscam entrar ou expandir sua presença no comércio eletrônico. Sua dedicação à qualidade, segurança e satisfação do cliente tem sido um pilar fundamental de sua trajetória de sucesso. A empresa está comprometida em proporcionar experiências de e-commerce seguras e eficientes, mantendo-se na vanguarda da tecnologia e das melhores práticas do setor.

2. Problema

Recentemente, uma das plataformas da BetaSoft foi alvo de uma injeção SQL, resultando na exposição de informações confidenciais dos clientes. O incidente de injeção SQL que afetou a BetaSoft revelou-se uma ameaça sofisticada que comprometeu a integridade do banco de dados de uma de suas plataformas de e-commerce. A injeção SQL permitiu que atacantes explorassem vulnerabilidades no sistema, obtendo acesso não autorizado a informações sensíveis dos clientes. Dados cruciais, como nomes, endereços, informações de cartões de crédito e histórico de compras, foram comprometidos.

A profundidade dessa violação não se limita apenas à exposição dos dados dos clientes. O incidente impactou diretamente a confiança construída pela BetaSoft ao longo dos anos, colocando em xeque sua reputação no mercado altamente competitivo de e-commerce. Além dos desafios operacionais imediatos, a empresa agora enfrenta possíveis implicações legais devido à potencial violação de dados sensíveis, adicionando uma camada adicional de complexidade à situação. A compreensão abrangente deste problema é essencial para desenvolver estratégias eficazes não apenas para a recuperação imediata, mas também para garantir uma postura mais resiliente e preventiva no futuro.

3. Solução com Segurança da Informação

Ao enfrentar a complexidade da injeção SQL, a BetaSoft adotou uma abordagem abrangente, incorporando diretrizes da ISO 27001 em sua estratégia de segurança. A implementação dessa norma internacional de segurança da informação não

apenas fortaleceu as defesas da empresa contra ameaças cibernéticas, mas também destacou seu comprometimento com padrões reconhecidos globalmente.

A BetaSoft reconhece a ISO 27001 como um alicerce sólido para o desenvolvimento de práticas de segurança robustas. Com isso, a auditoria de segurança minuciosa abordou as vulnerabilidades específicas relacionadas à injeção SQL e também alinhou os processos da empresa com os princípios e requisitos rigorosos da ISO 27001. Essa abordagem não apenas corrige vulnerabilidades imediatas, mas estabelece uma base sólida para a contínua melhoria e conformidade com as melhores práticas reconhecidas internacionalmente.

4. Análise de Risco

A análise de risco concentrou-se na injeção SQL como uma ameaça crítica, identificando ativos de informação, como dados dos clientes e informações estratégicas da empresa, em risco. Além disso, a falta de atualizações de softwares e revisões nas validações nos campos de entrada do usuário foram identificadas como vulnerabilidades significativas, tornando-se uma porta de entrada para ataques de injeção SQL.

A BetaSoft entende que a análise de risco contínua é essencial para manter a segurança cibernética eficaz. A identificação e avaliação constante de ameaças potenciais garantirão que a empresa esteja sempre um passo à frente no que diz respeito à segurança da informação.

4.1. Principais Características e Riscos de Injeção SQL

A injeção SQL apresenta várias características distintas e riscos significativos para a segurança de um sistema. Ao explorar entradas não validadas, manipulação de strings SQL e atuando em diferentes escopos, seus impactos potenciais são variados e substanciais.

1. **Entrada não validada:** a principal brecha ocorre quando um aplicativo aceita dados de entrada do usuário sem a devida validação. Esta vulnerabilidade permite que dados maliciosos sejam inseridos, levando a execução não autorizada de instruções SQL. A ausência de validação adequada abre portas para manipulação indevida e exploração da lógica de consulta do sistema.
2. **Concatenação de strings SQL:** a exploração da injeção SQL envolve frequentemente a inserção de instruções maliciosas através da concatenação de strings. Esta técnica manipula a lógica da consulta original, permitindo que

atacantes modifiquem o comportamento da consulta para alcançar seus objetivos maliciosos. A concatenação de strings torna-se uma vulnerabilidade quando não é tratada com a devida precaução.

3. **Escopo da injeção:** a amplitude da injeção SQL é notável, pois pode afetar uma variedade de operações no banco de dados. Desde consultas SELECT, INSERT, UPDATE e DELETE até procedimentos armazenados, a vulnerabilidade abrange diversas áreas do sistema. Essa versatilidade faz da injeção SQL uma ameaça ampla, capaz de comprometer diferentes aspectos do banco de dados.

4. **Impactos potenciais:** os impactos resultantes de uma injeção SQL bem-sucedida são vastos e severos. Acesso não autorizado a dados sensíveis é uma ameaça iminente, expondo informações confidenciais dos usuários. Além disso, a modificação ou exclusão de registros no banco de dados torna-se uma possibilidade real, comprometendo a integridade dos dados. A execução de comandos adicionais, incluindo procedimentos armazenados maliciosos, representa uma ameaça à funcionalidade do sistema. O vazamento de informações confidenciais adiciona uma dimensão crítica, impactando a privacidade dos usuários e a reputação da organização.

5. Implementação de Controles de Segurança

Para prevenir ou mitigar ataques por injeção SQL, a BetaSoft adotou medidas de segurança avançadas, visando fortalecer suas defesas contra essa ameaça específica. As estratégias implementadas incluem:

1. **Uso de declarações preparadas (com parâmetros):** priorização do uso de declarações preparadas em suas consultas SQL. Esse método garante que, mesmo quando dados de entrada contêm instruções SQL, um atacante não possa alterar a intenção original da consulta. Ao empregar parâmetros em vez de incorporar diretamente os dados nas consultas, a empresa estabelece uma camada adicional de segurança, reduzindo significativamente o risco de manipulação maliciosa.

2. **Escapar caracteres especiais:** a conscientização sobre a natureza especial de certos caracteres em instruções SQL levou a BetaSoft a implementar rigorosos mecanismos de escape. Isso assegura que caracteres com significados especiais sejam tratados adequadamente, mitigando a possibilidade de sua utilização em um ataque de injeção SQL. O cuidado na manipulação desses caracteres contribui para a integridade e segurança das consultas executadas no banco de dados.

3. **Validação de entrada:** a validação de entrada é uma linha de defesa crucial contra injeções SQL. Foram implementadas verificações rigorosas para

identificar e rejeitar entradas não autorizadas antes que elas alcancem as consultas SQL. Essa abordagem proativa minimiza as oportunidades para manipulação maliciosa e estabelece um controle eficaz na entrada de dados, protegendo a integridade das operações do banco de dados.

4. **Monitoramento e Registro**: mantendo um compromisso com a transparência e a detecção proativa, a BetaSoft incorporou um sistema abrangente de monitoramento e registro de atividades do banco de dados. Esse mecanismo permite identificar padrões incomuns e comportamentos suspeitos, fornecendo uma resposta imediata a potenciais ameaças. O registro detalhado das atividades do banco de dados não apenas serve como uma ferramenta de investigação, mas também como uma medida preventiva para identificar possíveis vulnerabilidades antes que possam ser exploradas.

6. Criação de Política de Segurança da Informação

Após um ataque por injeção SQL, é crucial fortalecer a segurança da informação. A Política de Segurança da Informação deve ser atualizada considerando o incidente:

- Análise Pós-Incidente
    - Investigação detalhada.
    - Avaliação de danos.
- Atualização da Política de Segurança da Informação
    - Revisão de vulnerabilidades de injeção SQL.
    - Reforço de monitoramento contínuo.
    - Ênfase na proteção de dados sensíveis.
- Treinamento e Conscientização
    - Treinamento específico sobre injeção SQL.
    - Simulações de ataques para capacitar colaboradores.
    - Atualizações regulares sobre ameaças.
- Gestão de Crises
    - Atualização e teste do plano de resposta a incidentes.
    - Procedimentos claros de comunicação transparente.

Integrando essas medidas, a BetaSoft estará mais preparada para prevenir futuros ataques, proteger seus ativos digitais e responder eficazmente a incidentes.

7. Auditoria e Plano de Contingência

A resposta estratégica da BetaSoft à injeção SQL envolveu uma série de medidas para fortalecer os controles de segurança em toda a infraestrutura. A realização de uma auditoria abrangente foi o primeiro passo, visando identificar não apenas as vulnerabilidades associadas à injeção SQL, mas também outros pontos de potencial exposição. Uma abordagem proativa permitiu a análise completa da postura de segurança, fornecendo percepções valiosas para a implementação de medidas preventivas e corretivas.

As atualizações regulares de software emergiram como uma prática crucial para a BetaSoft. A empresa reconhece a importância de manter todos os sistemas, frameworks e bibliotecas atualizados para mitigar vulnerabilidades conhecidas. Esse compromisso com a atualização constante não apenas corrige falhas de segurança, mas também contribui para uma postura de segurança mais resiliente frente às ameaças em constante evolução no cenário cibernético.

8. Conclusão

Ao enfrentar diretamente os desafios apresentados pela injeção SQL, a BetaSoft demonstra seu compromisso com a segurança cibernética. A integração de práticas específicas de prevenção em sua política de segurança da informação e a atualização contínua dos controles de segurança destacam a maturidade da empresa em lidar com ameaças emergentes. A BetaSoft está agora em uma posição mais resiliente para proteger os dados dos clientes, reconstruir a confiança e fortalecer sua posição no mercado.

Este capítulo na jornada de segurança da informação da BetaSoft não apenas aborda o incidente atual, mas estabelece as bases para um futuro mais seguro. A aprendizagem contínua e a adaptação são essenciais em um cenário de ameaças em constante evolução, e a BetaSoft está preparada para liderar nesse ambiente dinâmico.