**Relatório de Avaliação de Vulnerabilidade**

**Data:** 3º de Fevereiro de 2025

**Descrição do Sistema**

O servidor em análise é composto por um processador de alta performance e 128 GB de memória. Ele roda a versão mais recente do sistema operacional Linux e hospeda um sistema de gerenciamento de banco de dados MySQL. O sistema está configurado com uma conexão de rede estável utilizando endereços IPv4, permitindo interação com outros servidores na rede. Para garantir a segurança das transmissões de dados, são utilizadas conexões criptografadas via SSL/TLS.

**Escopo**

A avaliação de vulnerabilidade foca nos controles de acesso atuais do sistema. A análise abrange um período de três meses, de junho a agosto de 20XX, e segue as diretrizes estabelecidas pelo NIST SP 800-30 Rev. 1 para a avaliação de risco do sistema de informações.

**Objetivo**

O servidor de banco de dados é um sistema centralizado que armazena e gerencia grandes volumes de dados, incluindo informações sobre clientes, campanhas e dados analíticos. Esses dados são utilizados para rastrear o desempenho e personalizar as campanhas de marketing. A segurança desse sistema é crítica devido ao seu uso constante em operações de marketing, sendo essencial proteger as informações contra vazamentos ou alterações não autorizadas.

**Avaliação de Risco**

| **Fonte de Ameaça** | **Evento de Ameaça** | **Probabilidade** | **Gravidade** | **Risco** |
| --- | --- | --- | --- | --- |
| **Hacker** | Obtenção de informações sensíveis via exfiltração | 3 (Alta) | 3 (Alta) | 9 (Crítico) |
| **Funcionário** | Interrupção de operações críticas | 2 (Média) | 3 (Alta) | 6 (Alto) |
| **Cliente** | Alteração/Exclusão de informações críticas | 1 (Baixa) | 3 (Alta) | 3 (Moderado) |

A avaliação de risco considera as ameaças potenciais relacionadas à manipulação e ao armazenamento de dados sensíveis. A probabilidade de ocorrência de um incidente de segurança foi determinada com base nas permissões de acesso atuais do sistema. A gravidade dos incidentes foi medida levando em conta o impacto nas operações diárias da empresa.

**Abordagem**

A análise dos riscos envolveu a consideração de como os dados são armazenados e gerenciados no sistema. As fontes de ameaça foram identificadas com base na probabilidade de incidentes de segurança, levando em conta as permissões de acesso abertas e o nível de controle existente. A gravidade dos incidentes foi ponderada em relação ao impacto nas operações da empresa, com especial atenção para a perda ou vazamento de dados sensíveis.

**Estratégia de Remediação**

Para mitigar os riscos identificados, recomendamos a implementação das seguintes ações:

* **Controle de Acesso:** Implementar autenticação multifatorial (MFA) para garantir que apenas usuários autorizados possam acessar o sistema de banco de dados.
* **Autenticação e Autorização:** Utilizar senhas fortes e controles de acesso baseados em funções (RBAC) para restringir os privilégios de usuários de acordo com suas responsabilidades.
* **Criptografia de Dados:** Substituir o SSL por TLS para garantir que os dados em trânsito estejam devidamente criptografados.
* **Controle de Acesso por IP:** Implementar uma lista de IPs permitidos para restringir o acesso à base de dados apenas a escritórios corporativos, prevenindo conexões de usuários não autorizados da internet.
* **Auditoria e Monitoramento:** Estabelecer um sistema robusto de auditoria para monitorar e registrar todas as atividades de acesso ao banco de dados, ajudando a detectar atividades suspeitas.