Relatório de ameaça de vulnerabilidade

4st Outubro de 2025

Descrição do Sistema

O hardware do servidor consiste em um processador CPU poderoso e 128 GB de memória. Ele funciona na versão mais recente do sistema operacional Linux e hospeda um sistema de gerenciamento de banco de dados MySQL. Está configurado com uma conexão de rede estável usando endereços IPv4 e interage com outros servidores na rede. As medidas de segurança incluem conexões criptografadas SSL/TLS.

Escopo

O escopo desta avaliação de vulnerabilidade relaciona-se aos controles de acesso atuais do sistema. A avaliação abrangerá um período de três meses, de junho de 20XX a agosto de 20XX. O NIST SP 800-30 Rev. 1 é utilizado para orientar a análise de risco do sistema de informação.

Propósito

Considere as seguintes perguntas para ajudá-lo a escrever:
Como o servidor de banco de dados é valioso para o negócio?
Por que é importante para o negócio proteger os dados no servidor?
Como o servidor pode impactar o negócio se ele for desativado?

Avaliação de risco

Fonte de ameaça	Evento de ameaça	Probabilidade	Gravidade	Risco
Concorrente	*Obter informações sensíveis por meio de infiltração*	*1*	*3*	*3*

Funcionario Interno	*Vazamento acidental de dados por e-mail ou compartilhamento indevido*	*2*	*2*	*4*
Hacker externo	*Ataque de ransomware que criptografa o servidor de banco de dados*	*3*	*3*	*9*

Abordagem

Os riscos consideraram os métodos de armazenamento e gerenciamento de dados da empresa. A probabilidade de ocorrência de uma ameaça e o impacto desses eventos potenciais foram avaliados em relação aos riscos para as necessidades operacionais do dia a dia**.**

Estratégia de Remediação

Implementação de mecanismos de autenticação, autorização e auditoria para garantir que apenas usuários autorizados acessem o servidor de banco de dados. Isso inclui o uso de senhas fortes, controles de acesso baseados em funções e autenticação multifator para limitar os privilégios dos usuários. Criptografia de dados em trânsito usando TLS em vez de SSL. Lista de permissões de IP para escritórios corporativos, a fim de impedir que usuários aleatórios da internet se conectem ao banco de dados.