Relatório de avaliação de vulnerabilidade

24st Outubro 2024

Descrição do sistema:

O hardware do servidor consiste em um poderoso processador CPU e 128 GB de memória. Ele continua a versão mais recente do sistema operacional Linux e hospeda um gerenciamento de banco de dados MySQL no sistema. Ele é 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 está relacionado aos atuais controles de acesso do sistema. A avaliação abrangerá um período de três meses, de Outubro de 2024 a Janeiro de 2025. O NIST-SP 800-30 Rev. 1 é usado para orientar a análise de risco do sistema de informação.

Proposito

O servidor de banco de dados é um sistema de computador centralizado que armazena e gerencia grandes quantidades de dados. O servidor é usado para armazenar dados de clientes, campanhas e dados analíticos que podem ser posteriormente analisados para acompanhar o desempenho e personalizar os esforços de marketing. É fundamental garantir o sistema devido ao seu uso regular para operações de marketing.

Avaliação de risco

Fonte da ameaça	Evento da ameaça	Probabilidade	Gravidade	Risco
Hacker	*Obtenha informações confidenciais por meio de exfiltração.*	*3*	*3*	*9*
Funcionarios	*Interrompa operações de missão crítica*	*2*	*3*	*6*
Cliente	*Alterar/excluir informações críticas*	*1*	*3*	*3*

Abordagem

Os riscos medidos consideraram os procedimentos de armazenamento e gerenciamento de dados do negócio. Fontes e eventos de ameaças potenciais foram determinados usando a probabilidade de um incidente de segurança dadas as permissões de acesso aberto do sistema de informação. A gravidade dos incidentes potenciais foram avaliados em relação ao impacto nas necessidades operacionais diárias.

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, baseadas em funções, controles de acesso e autenticação multifator para limitar os privilégios do usuário. Criptografia de dados em movimento usando TLS em vez de SSL. Lista de permissões de IP para escritórios corporativos para evitar usuários aleatórios da Internet se conecte ao banco de dados.