Relatório de Avaliação de Vulnerabilidades

01 de julho de 2025

Descrição do Sistema

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Escopo

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Propósito

- O servidor de banco de dados é um ativo estratégico fundamental, cujo valor para o negócio transcende o hardware e o software. Ele representa o núcleo central onde as informações mais críticas da empresa são armazenadas, processadas e disponibilizadas.
- Proteger os dados hospedados neste servidor é crucial para a continuidade e o sucesso do negócio. Como o servidor abriga um banco de dados MySQL que é de suma importância para a operação do sistema, a segurança desses dados impacta diretamente três pilares essenciais: Confidencialidade, integridade e disponibilidade.
- Uma falha ou desativação deste servidor teria um impacto imediato e severo nas operações de negócio. Dado que ele executa um banco de dados MySQL essencial, sua indisponibilidade resultaria em: Interrupção operacional total, perdas financeiras diretas e danos à reputação e confiança

Avaliação de Riscos

Threat source	Threat event	Likelihood	Severity	Risk
Empresa Competidora	*Acesso a informações confidenciais por infiltração.*	*1*	*3*	*3*
Usuário Privilegiado	*Alteração e exclusão de dados confidenciais.*	*1*	*3*	*3*
Hacker	*Ataque DoS para interromper operações*	*3*	*3*	*9*

Abordagem

Nossa abordagem para esta avaliação qualitativa foi identificar um conjunto diversificado de ameaças de alto impacto que representam os riscos mais significativos para o negócio.Cada cenário representa um risco de negócio crítico, pois um comprometimento em qualquer um desses pilares poderia levar a perdas financeiras severas, paralisia operacional e danos à reputação. Este método fornece uma visão holística das principais ameaças que este ativo de servidor crítico enfrenta.

Estratégia de remediação

Para proteger o sistema, uma estratégia de defesa em profundidade é recomendada para mitigar os riscos identificados por meio de controles de segurança em camadas. Para combater ameaças internas e o acesso não autorizado, a implementação do princípio do menor privilégio e o fortalecimento da estrutura AAA (Authentication, Authorization, Accounting) são cruciais para garantir um registro robusto e permissões de usuário estritamente controladas. Além disso, a aplicação de autenticação multifator (MFA) para todo o acesso administrativo e a implantação de um serviço de mitigação de DoS baseado em nuvem reduzirão significativamente os riscos de exfiltração de dados e interrupção do serviço.