Relatório de Avaliação de Vulnerabilidades

1st Janeiro 20XX

Descrição do sistema

O hardware do servidor consiste em um processador CPU potente 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. 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 vulnerabilidades 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. A publicação **NIST SP 800-30 Rev. 1** é utilizada como guia para a análise de riscos do sistema de informação.

Objetivo

Considere as seguintes perguntas para ajudar na sua redação:

- ***Qual a importância do servidor de banco de dados para a empresa?***
  R.: O servidor de banco de dados hospeda todas as informações e dados da empresa, desde de funcionários internos a clientes com acessos externos.

- ***Por que é importante para a empresa proteger os dados no servidor?***
  R.: É essencial garantir a segurança do banco de dados no servidor, pois, dessa forma podemos evitar que os dados sejam acessados de forma indevida ou roubados por usuários mal-intencionados.

- ***Como o servidor impactaria os negócios se fosse desativado?***
  R.: Se o servidor fosse desativado, nenhum usuário conseguiria acessar suas informações, isso impactaria diretamente nas vendas e reputação da empresa, fazendo assim que houvesse uma cada exponencial de valor no mercado e de confiabilidade na empresa.

Avaliação de risco

Fonte de ameaça	Evento de ameaça	Probabilidade	Gravidade	Risco
Exemplo: Concorrente	*Obtenha informações confidenciais por meio de exfiltração.*	*1*	*3*	*3*
Interação com outros servidores - Hacker	*Caso outro servidor sofra um ataque com um malware do tipo worm, ransomware ou até a falsificação de certificados, o compartilhamento de informações poderia acarretar no roubo de informações e dados sigilosos do servidor da empresa por meio de um usuário mal-intencionado.* *Evento identificado: Fabricar certificados falsificados.*	*2*	*3*	*7*
Ataque utilizando DoS ou DDoS - Hacker	*Usuários externos mal-intencionados podem utilizar da conexão do servidor com a rede externa para "derrubar" seu serviços por meio de ataques com DoS ou DDoS, que sobrecarrega os servidor e trava o seu funcionamento.* *Evento identificado: Realizar ataques de negação de serviço (DoS).*	*2*	*3*	*9*

Abordagem

Os riscos considerados foram os métodos de armazenamento e gerenciamento de dados da empresa. A probabilidade de ocorrência de uma ameaça e o impacto desses eventos potenciais foram ponderados em relação aos riscos para as necessidades operacionais diárias. Limitar a interação do servidor com outros servidores identificados da empresa, a fim de evitar que um ataque se espalhe de forma catastrófica e realizar uma distribuição do tráfego da rede e manter os sistemas atualizados para minimizar a superfície deste tipo de ataque.

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. Restrição de IPs para escritórios corporativos a fim de impedir que usuários aleatórios da internet se conectem ao banco de dados.