SENAI – ETORE ZANINI

DARIO CESAR DE SANTANA

SA2 - Atividade 2 - online - Política de Qualidade

Prof. Tuon

SERTÃOZINHO

2021

Segurança do Banco de Dados

Uma realidade do gerenciamento de grandes organizações envolve a coleta de grandes quantidades de dados confidenciais que são armazenados e gerenciados em bancos de dados. Isso torna os bancos de dados um alvo principal para ataques cibernéticos. Neste tópico abordarei algumas práticas recomendadas de segurança de banco de dados que podem ajudar a manter um banco de dados protegidos contra invasores e comentarei duas destas práticas.

Servidores de banco de dados e servidores web separados

No sentido tradicional, isso significa manter seu servidor de banco de dados em um ambiente seguro e bloqueado, com controles de acesso em vigor para manter pessoas não autorizadas do lado de fora. Mas também significa manter o banco de dados em uma máquina física separada, removida das máquinas que executam aplicativos ou servidores da web.

Principais ferramentas de segurança de banco de dados.

Um servidor da web tem maior probabilidade de ser atacado, pois está localizado em uma DMZ e, portanto, acessível publicamente. E se um servidor da web for comprometido e o servidor de banco de dados for executado na mesma máquina, o invasor terá acesso como usuário root ao seu banco de dados e dados.

Acesso seguro do usuário ao banco de dados

Você deve ter como objetivo o menor número possível de pessoas para ter acesso ao banco de dados. Os administradores devem ter apenas os privilégios mínimos necessários para realizar seu trabalho e apenas durante os períodos em que precisam de acesso. Para organizações menores, isso pode não ser prático, mas no mínimo as permissões devem ser gerenciadas usando grupos ou funções, em vez de concedidas diretamente.

Se a organização for maior, deve se considerar automatizar o gerenciamento de acesso usando um software de gerenciamento de acesso. Isso pode fornecer aos usuários autorizados uma senha temporária com os privilégios de que precisam sempre que precisam acessar um banco de dados. Ele também registra as atividades realizadas durante esse período e evita que os administradores compartilhem senhas. Embora os administradores possam achar conveniente compartilhar senhas, fazer isso torna a segurança e a responsabilidade adequadas do banco de dados quase impossíveis.

Além disso, é aconselhável garantir que os procedimentos padrão de segurança da conta sejam seguidos:

_Senhas fortes devem ser aplicadas;

_Hashes de senha devem ser armazenados criptografados;

_As contas devem ser bloqueadas após três ou quatro tentativas de login;

_Um procedimento deve ser implementado para garantir que as contas sejam desativadas quando o pessoal sai ou muda para funções diferentes.

Atualize regularmente seu sistema operacional e patches

É importante atualizar regularmente seu sistema operacional e software de banco de dados com todos os patches de segurança instalados para proteção contra as vulnerabilidades descobertas mais recentemente. Deve também garantir que todos os controles de segurança do banco de dados fornecidos pelo banco de dados estejam ativados (a maioria é ativada por padrão), a menos que haja um motivo específico para a desativação. Isso é particularmente importante para bancos de dados conectados a um grande número de aplicativos de terceiros, cada um dos quais requer seus próprios patches.

Auditar e monitorar continuamente a atividade do banco de dados

Isso inclui o monitoramento de logins (e tentativas de logon) no sistema operacional e no banco de dados e a revisão dos logs regularmente para detectar atividades anômalas. Deve se também pode criar alertas para notificar os membros relevantes da equipe quando uma atividade potencialmente maliciosa é identificada.

O monitoramento eficaz deve permitir que você identifique quando uma conta foi comprometida, quando um funcionário está realizando atividades suspeitas ou quando seu banco de dados está sob ataque. Também deve ajudá-lo a determinar se os usuários estão compartilhando contas e alertá-lo se contas forem criadas sem sua permissão (por exemplo, por um hacker).

O software de monitoramento de atividade de banco de dados (DAM) pode ajudar com isso, fornecendo monitoramento que é independente do registro de banco de dados nativo e funções de auditoria; também pode ajudar a monitorar a atividade do administrador.

Teste a segurança do seu banco de dados

Depois de construir sua infraestrutura de segurança de banco de dados, você deve colocá-la contra um ataque real. Hackear ou auditar seu próprio banco de dados irá colocá-lo na mente de um invasor e ajudá-lo a encontrar vulnerabilidades que você possa ter perdido. Para garantir que o teste seja abrangente o suficiente, existem serviços terceirizados e hackers de chapéu branco especializados em testes de penetração que você pode contratar para fazer o trabalho por você.

Criptografar dados e backups

É um procedimento padrão em muitas organizações criptografar os dados armazenados. No entanto, é igualmente importante criptografar os dados em trânsito.

Você também deve fazer backup regularmente do seu banco de dados e garantir que todos os backups sejam criptografados e armazenados separadamente das chaves de descriptografia. Por

exemplo, você não deve armazenar backups criptografados ao lado de chaves de descrição em texto simples. O backup regular do sistema não protege apenas contra hackers, mas também contra outras falhas, como problemas com hardware físico.