Politica de qualidade

De acordo com o relatório do terceiro trimestre de 2020 da Risk Based Security , cerca de 36 bilhões de registros foram comprometidos entre janeiro e setembro de 2020. Embora esse resultado seja bastante surpreendente, ele também envia uma mensagem clara da necessidade de medidas eficazes de segurança de banco de dados.

As medidas de segurança de **banco de dados** são um pouco diferentes das práticas de segurança de sites . Segurança de **banco de dados** envolvem etapas físicas, soluções de software e até mesmo a educação de seus funcionários.

A seguir algumas práticas recomendadas de segurança de banco de dados que atuam para reforçar a segurança de dados confidenciais.

1. Implantar segurança de banco de dados físico

Os data centers ou seus próprios servidores podem ser suscetíveis a ataques físicos de terceiros ou mesmo a ameaças internas.

Para serviço de hospedagem na web, certifique-se de que seja uma empresa com um histórico conhecido de levar a sério as questões de segurança física . Também é melhor evitar serviços de hospedagem gratuitos devido à possível falta de segurança.

Para próprios servidores, é altamente recomendável adicionar medidas de segurança física, como câmeras, fechaduras e equipe de segurança, acesso aos servidores físicos deve ser registrado e concedido apenas a pessoas específicas, a fim de mitigar o risco de atividades maliciosas.

2. Servidores de banco de dados separados

Os bancos de dados exigem medidas de segurança especializadas para mantê-los protegidos contra ataques cibernéticos. Além disso, ter seus dados no mesmo servidor que seu site também os expõe a diferentes vetores de ataque que visam sites.

Para atenuar riscos de segurança, separe seus servidores de banco de dados de todo o resto. Além disso, use informações de segurança em tempo real e monitoramento de eventos (SIEM), que é dedicado à segurança do banco de dados e permite que as organizações tomem medidas imediatas no caso de uma tentativa de violação.

3. Configure um servidor proxy HTTPS

Um servidor proxy avalia as solicitações enviadas de uma estação de trabalho antes de acessar o servidor de banco de dados. De certa forma, este servidor atua como um gatekeeper que visa impedir a entrada de solicitações não autorizadas.

Ao lidar com informações confidenciais, como senhas, informações de pagamento ou informações pessoais, configure um servidor HTTPS. Dessa forma, os dados que trafegam pelo servidor proxy também são criptografados, fornecendo uma camada de segurança adicional.

4. Evite usar portas de rede padrão

Os protocolos TCP e UDP são usados ao transmitir dados entre servidores. Ao configurar esses protocolos, eles usam portas de rede padrão automaticamente .

As portas padrão são freqüentemente usadas em ataques de força bruta devido à sua ocorrência comum.

No entanto, ao atribuir uma nova porta, verifique o registro da porta da Autoridade para atribuição de números da Internet para garantir que a nova porta não seja usada para outros serviços.

5. Implantar protocolos de criptografia de dados

Criptografar seus dados não é importante apenas ao manter seus segredos comerciais ; também é essencial ao mover ou armazenar informações confidenciais do usuário.

A configuração de protocolos de criptografia de dados reduz o risco de uma violação de dados bem-sucedida. Isso significa que, mesmo que os cibercriminosos obtenham seus dados, essas informações permanecerão seguras.

6. Crie backups regulares de seu banco de dados

Embora seja comum criar backups de seu site, é essencial criar backups para seu banco de dados regularmente. Isso reduz o risco de perda de informações confidenciais devido a ataques maliciosos ou corrupção de dados.

Além disso, para aumentar ainda mais a segurança, certifique-se de que o backup seja armazenado e criptografado em um servidor separado. Dessa forma, seus dados são recuperáveis e seguros se o servidor de banco de dados primário ficar comprometido ou permanecer inacessível.

7. Use firewalls de banco de dados e aplicativos da web

Os firewalls são a primeira camada de defesa para impedir a entrada de tentativas de acesso mal-intencionado. Além de proteger seu site, você também deve instalar um firewall para proteger seu banco de dados contra diferentes vetores de ataque.

Existem três tipos de firewalls comumente usados para proteger uma rede:

Firewall de filtro de pacotes
Inspeção de estado de pacote (SPI)
Firewall do servidor proxy

Certifique-se de configurar seu firewall para cobrir quaisquer brechas de segurança corretamente. Também é essencial manter seus firewalls atualizados, pois isso protege seu site e banco de dados contra novos métodos de ataque cibernético.

CNPJ 30.998.352/0001-49