Segurança em Banco de dados: Integridade de dados

A principal característica de um sistema é controlar os processos de uma empresa. Dessa forma, cada solução que encontramos hoje no mercado de tecnologia possui características com objetivo de proporcionar aos clientes uma qualidade considerável em requisitos de segurança, performance, escalabilidade e, acima de tudo, coerência no uso da informação.

Esta coerência se trata de garantir que uma informação será verdadeira, será confiável e íntegra.

Quando um sistema controla os dados de uma organização, estes dados devem ser cuidadosamente analisados, afinal eles estarão de alguma forma interligados entre si no que diz respeito ao processo do negócio como um todo.

Por exemplo, um cadastro de fornecedores estará de alguma forma se comunicando com o cadastro de produtos, afinal os produtos pertencem a um fornecedor. Assim, a integridade de uma entidade pode ter impacto diretamente em outra entidade.

Normalmente cada funcionário tem um cargo e uma função; operar um sistema faz parte do dia a dia deste funcionário. Quando existe mais de um funcionário com a mesma função, eles utilizam o mesmo sistema e realizam os mesmos processos.

Isso pode parecer simples, porém se um sistema não tiver regras de integridade de dados, a forma de inserir os dados neste sistema ocorrerá de forma desordenada, causando um grande problema de registros sem uma regra definida ou mesmo inseridos de forma incorreta.

Podemos imaginar agora um ambiente de uma empresa que usa um sistema para controlar seus processos e, em um determinado momento, optam por criar um BI. Quando criamos um BI, partimos do princípio de que existe uma integridade na informação que será inserida neste BI.

Toda informação do sistema que controla a empresa será enviado por algum processo de ETL (ver **BOX 1**) para esse BI. Um sistema sem integridade de dados pode resultar em um BI não confiável e com uma informação falsa.

BOX 1. ETL

O Extract Transform Load dá nome às ferramentas que têm como função a extração de dados em diversos sistemas, fazem tratamentos e transformações nestes dados, para então inseri-los em DataWarehouses e Data Marts.

Geralmente este BI é consultado por diretores das empresas para apoiarem na tomada de decisões em várias esferas do negócio, e pode funcionar como um termômetro para medir se, por exemplo, um produto é viável ou não no mercado.

Podemos perceber que a falta de integridade na informação pode trazer danos irreversíveis para o negócio, podendo causar problemas de impactos financeiros.

Analistas, desenvolvedores, ADs e DBAs, consomem uma boa parte de seu tempo planejando como usar as regras de integridade de dados nos SGBDs de forma eficiente. Visando esta necessidade, demonstraremos neste artigo os mecanismos existentes para garantir a integridade da informação, e demonstraremos em exemplos práticos como implementar as regras no SQL Server e no Oracle.

Segurança em Banco de Dados: conheça as 5 principais causas de ataques

Atualmente, o maior bem que uma empresa possui é a informação. E, quando se trata de manter a confiabilidade dos próprios dados, são muitos os desafios enfrentados — sendo a segurança em banco de dados um dos maiores deles.

Por várias perspectivas, existem ameaças à integridade da informação que transita dentro de uma organização. Cabe, então, aos especialistas contratados moderar a ocorrência desse cenário e agir de forma concisa contra investidas não autorizadas.

Nesse sentido, é muito importante ter conhecimento sobre as principais brechas possíveis que podem existir nos bancos de dados empresariais. Por isso, continue lendo e veja as principais causas de ataques para que você se previna e não permita que isso aconteça na sua empresa!

5 principais causas de ataques a banco de dados

1. SQL Injection

O tipo mais conhecido de ataque a banco de dados é o SQL Injection. Nessa possibilidade, são incluídas instruções não autorizadas e mal-intencionadas no sistema, que podem dar os mais diversos privilégios ao agente invasor.

Um hacker que consegue acesso usando SQL Injection pode dar a si mesmo permissão total de manipulação das informações armazenadas, e causar um enorme estrago nos dados mal protegidos da empresa.

Existe ainda uma segunda categoria de ataques de injeção: o NoSQL Injection, que age em cima de soluções Big Data.

Assim, para que essas aberturas a acessos indevidos não aconteçam, os bancos devem estar muito bem codificados, com a segurança sempre em dia. A natureza dessas soluções já não utiliza nenhum comando SQL, impossibilitando o primeiro tipo de ataque.

2. Privilégios demais a pessoas demais

Controlar o que se pode acessar e quais ações podem ser realizadas em cima das informações é uma parte básica da segurança em banco de dados. Contudo, existem empresas que ainda não se preocupam com esse risco.

Se muitas pessoas têm acessos a dados sensíveis ou ao ambiente de produção, por exemplo, é muito possível — mesmo que de forma não intencional — que um colaborador delete informações que vão parar o funcionamento de vários sistemas.

E isso pode acarretar em um prejuízo financeiro de forma imediata a empresa. Além do problema do dinheiro, o tempo que será gasto pelo DBA para “apagar esse incêndio” será outro prejuízo em grande escala.

Afinal, uma situação dessas atrasa todos os outros projetos evolutivos em andamento, impedindo a empresa de crescer por uma total falta de cuidado com seu ativo mais precioso.

3. Deficiência na auditoria

Quando novas tabelas, ou mesmo campos são criados em um banco de dados, eles devem passar por um processo extremamente rigoroso de auditoria. Não se pode deixar passar nada, pois um simples erro, como um caractere a menos em um campo, já pode parar o sistema de forma geral.

E como ninguém deveria poder alterar um banco em horários não planejados, isso pode fazer com que durante o restante do dia os funcionários não possam trabalhar mais nos sistemas que acessam o banco de dados.

Caso a empresa não possua recursos ou conhecimento suficiente para garantir a integridade do banco de dados, é interessante terceirizar esse serviço, deixando que profissionais especializados cuidem da saúde do sistema e impedindo que cenários de bloqueio do trabalho de outras áreas **ocorra.**

4. Sistemas de segurança fracos e/ou desatualizados

Um erro muito comum que os usuários cometem nas empresas é ter senhas fáceis, ou até manter as senhas padrão em seu acesso. E, a partir de uma falha como essas, todos podem sair perdendo.

A importância de fortificar a senha deve ser muito bem esclarecida a todos, mesmo aos que não possuem conhecimentos de segurança.

Nesse sentido, os firewalls e as políticas de bloqueio e exceção devem ser sempre atualizadas, e técnicos com alta capacidade devem ser mantidos para cuidar dessa atividade. Até porque nenhum sistema é completamente livre de invasões.

Tecnologias que já estão ultrapassadas, com certeza, já foram destrinchadas por hackers e são mais vulneráveis a quem possui esse tipo de conhecimento.

Justamente por isso, são lançadas, periodicamente, novas versões de programas de proteção, que buscam estar sempre à frente de ataques — e esse ciclo continuará. Logo, para manter seguros seus dados, é preciso usar programas confiáveis, pessoas competentes e manter as atualizações em dia.

5. Exposição de mídia storage

Muitos casos de ataques também ocorrem a backups mal protegidos, e não à base principal de uma corporação. Por isso, quando são feitos backups do banco de dados, é extremamente importante lembrar que a segurança da mídia storage deve ser, pelo menos, igual à do servidor original.

Inclusive, o cuidado com essa tarefa deve ser o mesmo, pois faz parte de atividades que sempre serão realizadas. Assim, uma boa solução é realizar os backups na nuvem, pois a segurança nesse ambiente está sempre à frente em termos de novas tecnologias.

Caso sejam escolhidos backups locais, o processo a seguir deve ser definido e auditado, pois uma cópia da base mal protegida já é uma porta de entrada para quem quer prejudicar sua empresa.

Como cuidar da segurança em banco de dados da sua empresa

É trabalho dos responsáveis pela empresa zelar pela segurança das informações que pertencem a ela. E, para realizar isso com sucesso, é essencial ter um time de alta competência — seja ele próprio ou terceirizado.

Ter conhecimento sobre as tecnologias que garantem maior segurança e saber que isso tem um custo a arcar são atitudes que dão aos gerentes e líderes mais confiança para garantir a integridade dos dados.

Além disso, é sempre importante lembrar, os gastos com a proteção do banco de dados, com certeza, serão menores que os prejuízos de uma invasão, um roubo ou um vazamento de informações cruciais para o negócio.

O armazenamento acaba se tornando parte fundamental do corpo de uma empresa, pois registrar todo o histórico do negócio é fundamental para seus planos futuros. Por isso, investir na segurança em banco de dados é parte essencial do crescimento empresarial saudável e da busca por se destacar no mercado!

E aí, gostou do post? Essas dicas sobre como proteger seu banco de dados foram úteis? Então, aproveite agora para assinar a nossa newsletter e continue por dentro de muitos outros assuntos do mundo da tecnologia!

Conceitos sobre Segurança em Banco de Dados

Os bancos de dados são utilizados para armazenar diversos tipos de informações, desde dados sobre uma conta de e-mail até dados importantes da Receita Federal. A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade. Um Sistema gerenciador de banco de dados deve fornecer mecanismos que auxiliem nesta tarefa.

Os bancos de dados SQL implementam mecanismos que restringem ou permitem acessos aos dados de acordo com papeis ou roles fornecidos pelo administrador. O comando GRANT concede privilégios específicos para um objeto (tabela, visão, seqüência, banco de dados, função, linguagem procedural, esquema ou espaço de tabelas) para um ou mais usuários ou grupos de usuários.

A preocupação com a criação e manutenção de ambientes seguros se tornou a ocupação principal de administradores de redes, de sistemas operacionais e de bancos de dados. Pesquisas mostram que a maioria dos ataques, roubos de informações e acessos não- autorizados são feitos por pessoas que pertencentes à organização alvo.

Por esse motivo, esses profissionais se esforçam tanto para criar e usar artifícios com a finalidade de eliminar os acessos não-autorizados ou diminuir as chances de sucesso das tentativas de invasão (internas ou externas). Os controles de acesso em sistemas de informação devem certificar que todos os acessos diretos ao sistema ocorram exclusivamente de acordo com as modalidades e as regras pré-estabelecidas, e observadas por políticas de proteção.

De modo geral, os mecanismos de segurança referem-se às regras impostas pelo subsistema de segurança do SGBD, que verifica todas as solicitações de acesso, comparando-as com as restrições de segurança armazenadas no catálogo do sistema. Entretanto existem brechas no sistema e ameaças externas que podem resultar em um servidor de banco de dados comprometido ou na possibilidade de destruição ou no roubo de dados confidenciais.

As ameaças aos bancos de dados podem resultar na perda ou degradação de alguns ou de todos os objetivos de segurança aceitos, são eles: integridade, disponibilidade, confidencialidade. A integridade do banco de dados se refere ao requisito de que a informação seja protegida contra modificação imprópria.

A disponibilidade do banco de dados refere-se a tornar os objetos disponíveis a um usuário ou a um programa ao qual eles têm um direito legitimo. A confidencialidade do banco de dados se refere à proteção dos dados contra a exposição não autorizada. O impacto da exposição não autorizada de informações confidenciais pode resultar em perda de confiança pública, constrangimento ou ação legal contra a organização.

Controle de Acesso

É todo controle feito quanto ao acesso ao BD, impondo regras de restrição, através das contas dos usuários. O Administrador do BD (DBA) é o responsável superior por declarar as regras dentro do SGBD. Ele é o responsável por conceder ou remover privilégios, criar ou excluir usuários, e atribuição de um nível de segurança aos usuários do sistema, de acordo com a política da empresa.

Controle de Inferência

É um mecanismo de segurança para banco de dados estatísticos que atua protegendo informações estatísticas de um individuo ou de um grupo. Bancos de dados estatísticos são usados principalmente para produzir estatísticas sobre várias populações.

O banco de dados pode conter informações confidenciais sobre indivíduos. Os usuários têm permissão apenas para recuperar informações estatísticas sobre populações e não para recuperar dados individuais, como, por exemplo, a renda de uma pessoa específica.

Controle de Fluxo

É um mecanismo que previne que as informações fluam por canais secretos e violem a política de segurança ao alcançarem usuários não autorizados. Ele regula a distribuição ou fluxo de informação entre objetos acessíveis. Um fluxo entre o objeto A e o objeto B ocorre quando um programa lê valores de A e escreve valores em B. Os controles de fluxo têm a finalidade de verificar se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção. Dessa maneira, um usuário não pode obter indiretamente em B aquilo que ele ou ela não puder obter diretamente de A.

Criptografia de Dados

Você pode ler aqui um pouco mais sobre criptografia. É uma medida de controle final, utilizada para proteger dados sigilosos que são transmitidos por meio de algum tipo de rede de comunicação. Ela também pode ser usada para oferecer proteção adicional para que partes confidenciais de um banco de dados não sejam acessadas por usuários não autorizados. Para isso, os dados são codificados através da utilização de algum algoritmo de codificação. Assim, um usuário não autorizado terá dificuldade para decifrá-los, mas os usuários autorizados receberão chaves para decifrar esses dados. A criptografia permite o disfarceda mensagem para que, mesmo com o desvio da transmissão, a mensagem não seja revelada.

Usuários

Abrange usuários e esquema do banco de dados onde cada banco de dados Oracle tem uma lista de nomes de usuários. Para acessar um banco de dados, um usuário deve usar um aplicativo desse tipo e

tentar uma conexão com um nome de usuário valido. Cada nome tem uma senha associada para evitar o uso sem autorização.

Devem ser implementados ainda diferentes perfis de usuário para diferentes tarefas no Oracle, tendo em vista que cada aplicação/usuário tem a sua necessidade de acesso. Existe ainda a possibilidade de proteger os perfis com senha, o que é uma excelente medida. Além dessas medidas, o uso de cotas aumenta a restrição de espaço em disco a ser utilizado por usuários/aplicativos.

Domínio de Segurança

Onde cada usuário tem um domínio de segurança, um conjunto de propriedades que determinam coisas como ações (privilégios e papeis) disponíveis para o usuário; cota de tablespaces (espaço disponível em disco) do usuário; limites de recursos de sistema do usuário.

As tabelas (tablespaces) do sistema, como a system, devem ser protegidas de acessos de usuários diferentes dos usuários de sistema. A liberação de escrita e alteração de dados em tais tabelas é muito comum em ambientes de teste, onde os programadores e DBAs tomam tal atitude para evitar erros de aplicação por falta de privilégios. Porém, em ambientes de produção, tal medida é totalmente desaconselhável.

Autoridade

As autoridades fornecem um método de agrupar privilégios e controlar o nível de acesso dos administradores e operadores da base de dados com relação à manutenção e operações permitidas.As especificações da base de dados estão armazenadas em catálogos da própria base de dados. As autoridades do sistema estão associadas a membros de grupos e armazenados no arquivo de configuração administrativa do banco de dados. Este arquivo define as concessões de acesso e o que poderá ser executado de acordo com cada grupo.

Privilégios

Os privilégios são permissões únicas dadas a cada usuário ou grupo. Eles definem permissões para tipos de autorização. Pelos privilégios é possível autorizar o usuário a modificar ou alcançar determinado recurso do Banco de Dados.

Os privilégios também são armazenados em catálogos do próprio Banco de Dados, visto que os grupos de autoridade por já possuírem grupos predefinidos de privilégio concedem implicitamente privilégios a seus membros.

Tipos de privilégios discricionários

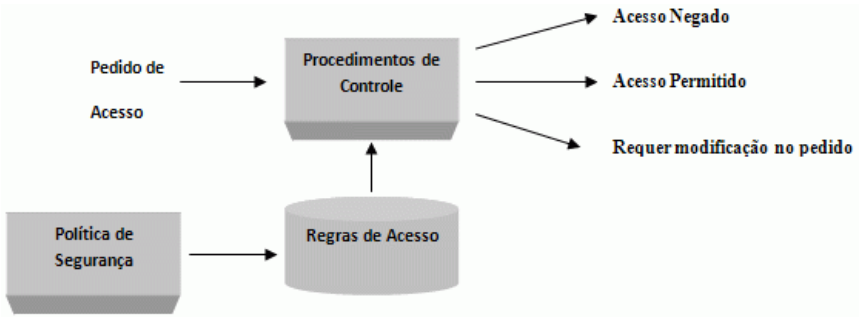
O SGBD deve oferecer acesso seletivo a cada relação do banco de dados baseando-se em contas específicas. As operações também podem ser controladas; assim, possuir uma conta não necessariamente habilita o possuidor a todas as funcionalidades oferecidas pelo SGBD. Informalmente existem dois níveis para a atribuição de privilégios para o uso do sistema de banco de dados:

- O nível de conta: Nesse nível, o DBA estabelece os privilégios específicos que cada conta tem, independente das relações no banco de dados.

- O nível de relação (ou tabela): Nesse nível, o DBA pode controlar o privilégio para acessar cada relação ou visão individual no banco de dados.

Revogação de Privilégios

Em alguns casos, interessa conceder um privilégio temporário a um usuário. Por exemplo, o proprietário de uma relação pode querer conceder o privilégio SELECT a umusuário para uma tarefa específica e depois revogar aquele privilégio quando a tarefa estiver completada. Por isso, é necessário um mecanismo para a revogação de privilégios. Em SQL, um comando REVOKE é introduzido com o intento de cancelar privilégios.



Sistema de Controle de Acesso

Controle de acesso obrigatório e para segurança multi-nível

Neste método, o usuário não tem um meio termo, ou ele tem ou não tem privilégios, sendo utilizado normalmente em BD que classificam dados de usuários, onde é necessário um nível a mais de segurança. A maioria dos SGBDs não oferecem esse tipo de controle de acesso obrigatório, ficando com os controles discricionários ditos anteriormente. Normalmente são utilizados em sistemas governamentais, militares ou de inteligência, assim como industriais e corporativas.

As **classes de segurança** típicas são altamente sigilosas (top secret, TS), secreta (secret, S), confidenciais (confidential) (C) e não Classificada (unclassified, U), em que TS é o nível mais alto e U é o mais baixo.

De uma forma geral, os mecanismos de controle de acesso obrigatório impõem segurança multinível, pois exigem a classificação de usuários e de valores de dados em classes de segurança e impõem as regras que proíbem o fluxo de informação a partir dos níveis de segurança mais altos para os mais baixos.

Controle de acesso baseado em papéis

É uma abordagem para restringir o acesso a usuários autorizados e uma alternativa aos sistemas de controles de acesso do tipo MAC e DAC. O conceito de controle de acesso baseado em papéis surgiu com os primeiros sistemas computacionais multiusuários interativos. A idéia central do RBAC é que permissões de acesso são associadas a papéis, e estes papéis são associados a usuários. Papéis são criados de acordo com os diferentes cargos em uma organização, e os usuários são associados a papeis de acordo com as suas responsabilidades e qualificações. Vários indivíduos podem ser designados para cada papel. Os privilégios de segurança comuns a um papel são concedidos ao nome dele, e qualquer indivíduo designado para esse papel automaticamente teria esses privilégios concedidos.

Os usuários podem ser facilmente remanejados de um papel para outro. Mudanças no ambiente computacional, como instalação de novos sistemas e remoção de aplicações antigas, modificam apenas o conjunto de permissões atribuídas aos diferentes papeis, sem envolver diretamente o conjunto de usuários.

A separação de tarefas é um requisito importante em diversos SGDBs. É necessária para impedir que um usuário realize sozinho o trabalho que requer o envolvimento de outras pessoas. A exclusão mútua de papéis é um método que pode ser implementado com sucesso.

Outro aspecto relevante nos sistemas RBAC são as restrições temporais possíveis que podem existir nos papéis, como o tempo e a duração das ativações de papéis e o disparo temporizado de um papel por uma ativação de outro papel. O uso se um modelo RBAC é um objetivo altamente desejado pela para solucionar os principais requisitos de segurança das aplicações baseadas na web.

Controle de acesso utilizando Triggers

Com a utilização das Triggers é possível criar mecanismos de segurança mais complexos que podem ser disparados cada vez que um evento é chamado. O comando *Insert* na tabela é exemplo de um evento que pode ser usado para disparar uma *Triggers*, além disso, as mesmas podem ser disparadas antes ou depois de comando especificado com o objetivo de prover maior rigor no controle de segurança.

Se o comando executado pelo usuário não for validado pela *Triggers*, um erro é sinalizado do corpo da própria *Triggers* para impedir que a tabela seja modificada indevidamente.

Controle de acesso utilizando Views

As *views* constituem um outro método de controle de acesso, normalmente utilizadas para restringir o acesso direto aos dados. Com a *view* é possível permitir acesso de usuário concedendo privilégios, ocultar linhas e colunas de informações confidenciais ou restritas residentes na tabela original das indicações do SQL.

Os privilégios e concessões são definidos somente na *view* e não afetam a tabela base sendo o acesso dos usuários delimitado pela view, a qual é gerada criando um subconjunto de dados na tabela referenciada.