Segurança em Servidores com Banco de Dados *Microsoft* SQL *Server*: Meios de Proteção contra invasões

Edison de Azevedo Filho
Uniandrade – PR
edison_filho@hotmail.com

Maria Claudia Lara da Costa
Faculdades OPET – PR
mclaudialara@gmail.com

RESUMO

Este artigo aborda a questão da segurança em Banco de Dados Microsoft SQL Server, no intuito de contribuir academicamente para o registro teórico do tema, enfatizando a diferença entre segurança e integridade de banco de dados e as principais vulnerabilidades de um SGBD, apontando ainda as medidas básicas de segurança a se tomar com relação a tais ameaças.

Palavras-chave: banco de dados, SQL, segurança, integridade

1. INTRODUÇÃO

A figura do administrador de dados no início dos anos 70 era uma das mais importantes dentro de uma empresa (CASH,1992). Diante da relevância e credibilidade de seu trabalho, todo processo decisório passou a ser submetido à sua verificação e aprovação antes de se chegar a um veredicto final. Se houvesse uma reunião da alta cúpula para tratar de metas para o próximo ano, por exemplo, seguramente o administrador de dados estaria presente para melhor planejar a organização dos dados para desta forma auxiliar a gestão do negócio, como grande conhecedor do negócio da organização.

O que ocorreu foi a adoção da TI[1] como suporte de negócios, de modo que sua efetiva utilização tornou-se imperativa para a estratégia e até mesmo para a sobrevivência das organizações (PORTER, 1999). Conforme ressalta Marcovitch (1999) estratégias empresariais, tecnológicas e de informação tornaram-se sistemas indissociáveis e interdependentes.

Instaurava-se uma tendência de valorização crescente de bases de dados bem organizadas e administradas, reforçada pela informatização das empresas em geral, dando início a uma busca pela estruturação centralizada de informações que requeria uma robustez no gerenciamento dos dados. A Era da Informação (CASTELLS,1999) elegia um de seus profissionais-ícones, e lhe impunha um desafio instigador: encontrar modos seguros do trato de Bancos de Dados.

Se vivemos hoje uma época onde o armazenamento e transmissão de dados valem ouro, ainda mais importante que eles é a capacidade de mantê-los protegidos, de modo que a questão da segurança em SGBDs[2] tornou-se o centro das preocupações do mercado da TI – uma tendência ainda com poucas repercussões no meio acadêmico. Diante disso, pretende-se

[1] TI – Tecnologia da Informação.
[2] SGBD – Sistema de Gerenciamento de Banco de Dados.

aqui elencar as principais ameaças da atualidade a banco de dados SQL[3] bem como técnicas básicas de defesa, de modo a contribuir para os registros teóricos deste importante tema que é a segurança em BD[4].

2. INTEGRIDADE E SEGURANÇA EM SISTEMAS DE BANCOS DE DADOS

Sabe-se que sistemas de gerenciamento de bancos de dados são caracterizados por sua habilidade de admitir o acesso eficiente a grandes quantidades de dados, garantindo-lhe durabilidade (GARCIA-MOLINA, 2000). Porém, mais do que sua organização, outros aspectos passaram a ser determinantes para a perenidade de um sistema. Como já dito por Tarandach[5] questões como segurança e integridade começaram a ter destaque, pois com o crescimento dos bancos de dados, seus esquemas de integração ficaram mais complexos e a tendência à falhas e erros também cresceu progressivamente.

Para o pleno entendimento da questão, é importante ressaltar a diferença entre os conceitos de segurança e integridade de dados. Date (2000) associa a noção de *Segurança* à proteção de dados contra revelação, alteração ou destruição não autorizada enquanto *Integridade* se refere à exatidão ou validade desses dados. Ambos estão ligados à idéia de proteger o BD, mas especificamente no caso da integridade, o foco não está em invasores externos, e sim em restringir o acesso a usuários internos, ou seja, garantir que os critérios de permissão de acesso sejam plenamente respeitados segundo aquilo que foi programado pelo DBA[6].

> "*As regras de integridade fornecem a garantia de que mudanças feitas no banco de dados por usuários autorizados não resultem em perda da consistência dos dados. Assim, as regras de integridade protegem o banco de dados de danos acidentais*"(SILBERSCHATZ,1999:191).

Já a segurança, de modo geral, refere-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 há várias vulnerabilidades do sistema e ameaças externas a ele que podem resultar em um servidor de banco de dados comprometido ou na possibilidade de destruição ou no roubo de dados confidenciais.

As diversas brechas de um SGBD (figura 1) apontam para a realidade de que um servidor de BD, por sua complexidade e importância, deve ser muito bem configurado e administrado segundo preocupações específicas. Para melhor entendimento da questão, na figura a seguir simula-se uma rotina de uso de uma Aplicação e um Banco de Dados apontando os principais ataques a que o sistema está sujeito para discussão detalhada de cada item.

---

[3] SQL (*Structured Query Language*) refere-se a uma linguagem para ambiente relacional, utilizável em numerosas aplicações, podendo manipular objetos de diferentes classes entre as funções de um Sistema de Gerenciamento de Banco de Dados (SGBD). Consagrada através da IBM, tornou-se uma das linguagens mais populares e amplamente utilizadas em Bancos de Dados principalmente por sua facilidade de manipulação e entendimento (MACHADO, 2004:315-317) sendo a linguagem mais utilizada do mercado (SILBERSCHATZ,1999:109).

[4] BD – Banco de Dados.

[5] IZAR TARANDACH (2007) é especialista em segurança de banco de dados e diretor de engenharia de sistemas da Guardium Inc. e está terminando seu programa de mestrado em segurança da informação na Boston University.

[6] DBA – *Data Base Administrator, termo utilizado para a função de* Administrador de Banco de Dados na área de tecnologia, inclusive no Brasil.

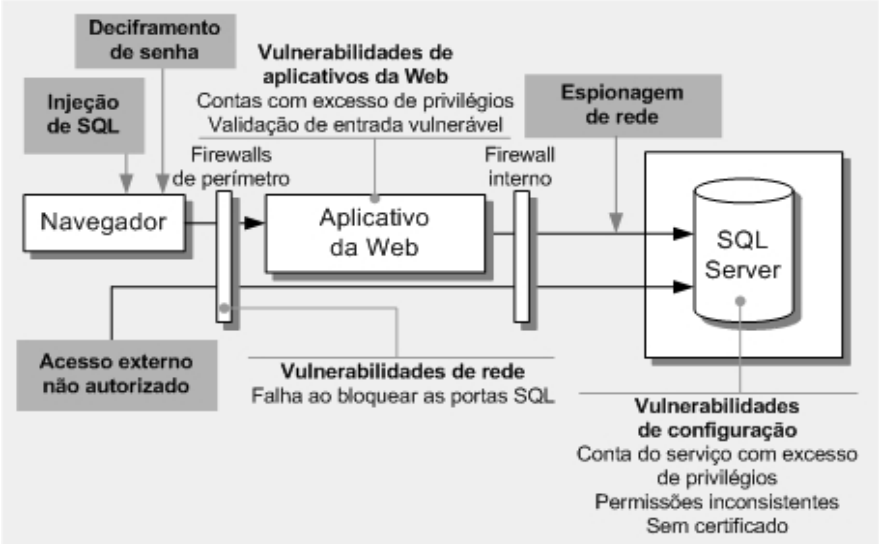

Figura1. Principais ameaças ao servidor de BD segundo a Microsoft (www.microsoft.com).

2.1 INCLUSÃO DE CÓDIGO SQL

Como Date menciona (DATE,2000:77), a maioria dos produtos de SQL permite que as instruções SQL sejam executadas diretamente – ou seja, interativamente de um terminal *on-line*. Com um ataque de inclusão de código SQL, o invasor explora as vulnerabilidades do código de acesso a dados e da validação da entrada do aplicativo para executar comandos arbitrários no banco de dados que usa o contexto de segurança do aplicativo da *Web*[7]. Nesse nível de ataque, explora-se principalmente a validação da entrada ineficaz nos aplicativos da *Web*; comandos SQL construídos de forma dinâmica e sem segurança; *logons*[8] de aplicativo com muitos privilégios ou permissões de baixa segurança que falham ao restringir o *logon* do aplicativo no banco de dados.

Para combater tentativas de ataques desta natureza, a primeira medida a se tomar é restringir e corrigir os dados de entrada no aplicativo antes de usá–los em consultas SQL.

Somente parâmetros SQL de tipo seguro devem ser usados para acesso aos dados, priorizando procedimentos armazenados ou seqüências de caracteres de comando SQL construídas de forma dinâmica. O uso de parâmetros SQL garante que os dados de entrada sejam submetidos a verificações de tipo e comprimento e que o código injetado seja tratado como dado literal, e não como instrução executável no banco de dados.

Um modo de garantir tal proteção é fazer uso de SQL-DDL[9]. Esta linguagem proporciona comandos para a definição de esquemas de relações, exclusão de relações, criação de índices e modificação nos esquemas de relações, segundo especificação de regras de integridade que os dados armazenados no banco de dados devem satisfazer. Com isso, atualizações que tentem violar as regras de integridade são desprezadas (SILBERSCHATZ,1999:110).

Outra medida é usar o *logon* do SQL *Server* com permissões restritas no banco de dados. Preferencialmente, deve-se conceder permissões de execução somente aos

---

7 *WEB* - Sistemas de documentos em hipermídia que são interligados e executados na Internet.

8 Logon é um conjunto de caracteres solicitado para os usuários que por algum motivo necessitam acessar algum sistema computacional.

9 DDL: *Data Definition Language* (Linguagem de Definição de Dados).

procedimentos armazenados e selecionados no banco de dados e não fornecer acesso direto à tabela.

2.2 ESPIONAGEM NA REDE

A arquitetura de implantação da maioria dos aplicativos inclui uma separação física entre o código de acesso a dados e o servidor de banco de dados. Conseqüentemente, os dados confidenciais, como dados específicos do aplicativo ou credenciais de logon de banco de dados, devem ser protegidos contra a espionagem na rede. As principais brechas que permitem ataques deste nível referem-se a canais de comunicação desprotegidos e à transmissão de credenciais em texto não criptografado para o banco de dados, como por exemplo, quando do uso da autenticação do SQL em vez da autenticação do *Windows*[10] ou da autenticação do SQL sem um certificado de servidor.

Para combater tais ameaças, deve-se utilizar a autenticação própria do *Windows* para estabelecer conexão com o servidor de banco de dados e impedir o envio de credenciais por meio da rede e instalar um certificado de segurança no servidor de banco de dados. Isso resultará na criptografia automática das credenciais SQL na rede. Para isso, é fundamental manter uma conexão SSL[11] entre o servidor *Web* e o servidor de banco de dados para proteger os dados confidenciais do aplicativo**.**

2.3 ACESSO NÃO AUTORIZADO AO SERVIDOR

Todo acesso direto ao servidor de banco de dados deve ser restrito a computadores cliente específicos para impedir conexões não autorizadas.

> "*Para que o dado fique protegido do uso indevido de qualquer usuário, a linguagem SQL permite a definição dos privilégios que cada um pode ter em relação às tabelas criadas no banco de dados. Os privilégios garantem a segurança e a integridade dos dados, bem como a responsabilidade de cada usuário sobre seus dados específicos*" (MACHADO, 2004:378).

Ao determinar os privilégios de acesso dos clientes, deve-se evitar falhas na configuração das portas do SQL Server no *firewall*[12] e atentar para as diretivas de filtragem IPSec.

Segundo Kent e Atkinson (1998), o IPsec é um protocolo de tunelamento que cria uma conexão especial entre dois pontos, assemelhando-se a um túnel. Nele, a extremidade iniciadora encapsula os pacotes da rede privada para o trânsito através da Internet, utilizando-se do protocolo TCP/IP (*Transmition Control Protocol / Internet Protocol*). Este refere-se a um conjunto de protocolos de comunicação entre computadores em rede.

Os filtros que devem ser aplicados no IPsec podem ser a autorização de um endereço IP ou uma range de IPs de origem/destino específicos, assim como portas específicas de origem/destino.

Quando se trata de acesso ao servidor, toda cautela é necessária, uma vez que tanto usuários autenticados como usuários sem nome e sem senha estão sujeitos a ataques de conexão direta. A exemplo disso, um invasor pode estabelecer uma conexão direta com o SQL Server e tentar obter resultados (informações) utilizando-se de ferramentas como o

---

10 *Windows*: Sistema Operacional desenvolvido pela *Microsoft*.

11 SSL: *Secure Sockets Layer*, são protocolos criptográficos que provêem comunicação segura na Internet para serviços como e-mail, navegação por páginas e outros tipos de transferência de dados.

12 *Firewall*: Segundo (Chapman e Zwicky, 1995) *firewall* é definido como "um componente ou conjunto de componentes que restringem o acesso entre uma rede protegida e a Internet, ou entre outros conjuntos de redes".

Analisador de Consultas (Isqlw.exe), ou o equivalente da linha de comando (Osql.exe), ou ainda, enviar pacotes construídos cuidadosamente para portas de escuta para obter informações do servidor, como sua versão de software.

Para combater esses ataques é preciso que as portas do SQL Server não sejam vistas de fora da rede de perímetro, e que dentro do perímetro o acesso direto de hosts não autorizados seja restrito, por exemplo, através de filtros IPSec ou TCP/IP.

2.4 QUEBRA DE SENHA

Uma primeira linha de ataque comum é tentar quebrar as senhas de nomes de conta conhecidos, como *sa* (a conta do administrador do SQL Server). Neste quesito, as vulnerabilidades comuns que levam a quebras de senha são geralmente o uso de senhas de baixa segurança (ou em branco) e senhas que contêm palavras comuns.

Há programas (*cracks*) que usam dicionários como método de ataque relacionado a tentativas repetitivas de seleção de palavras existentes para descobrir senhas. Aplicam, inclusive, regras combinatórias de forma a prever alterações em palavras que visem a tornar as senhas mais difíceis, como: "*shifts*", uso de maiúsculas, acréscimo de caracteres não alfa-numéricos e substituição de letras por algarismos.

Os ataques mais comuns de quebra de senha baseiam-se neste tipo de ataque de dicionário ou na detecção manual de senha. Para combater tais tentativas, é fundamental criar senhas para as contas de logon do SQL Server que atendam a requisitos de complexidade mínima e evitar o uso de senhas que contenham palavras comuns encontradas no dicionário.

Ao utilizar a autenticação do Windows, a complexidade da senha poderá ser aplicada pela diretiva de segurança do sistema operacional.

3. CHECKLIST DE PROTEÇÃO DO SQL SERVER

Pode ser difícil proteger bancos de dados, especialmente quando encontram-se online (Internet), uma vez que ficam permanentemente expostos a exame público. Uma "solução" interessante é a introdução erros deliberados em sua programação. A colocação de erros deliberados e omissões em um programa é conhecida como uma espécie de colocação de "sementes" dentro do banco de dados. É uma medida útil em casos de cópia ilegal para comprovação de autoria e originalidade, mas paliativa somente para casos de cópia.

Como a preocupação com a proteção de dados vai além da questão de duplicação do BD, torna-se fundamental o estabelecimento de um checklist básico para conferência dos principais elementos do servidor. Nesse sentido, há algumas categorias de configuração (figura 2) recomendadas obtidas em experiências reais, na validação de clientes e em estudos de implantações de segurança, que devem ser verificadas.

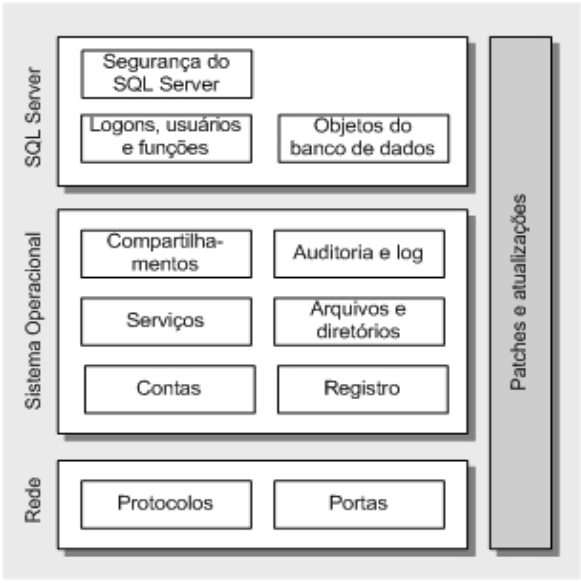

Figura 2. Categorias de segurança do servidor de banco de dados segundo a Microsoft (www.microsoft.com).

3.1 SQL SERVER

Usuários (e aplicativos) obtêm acesso ao SQL Server por meio do logon do servidor SQL. O logon está associado a um usuário do banco de dados e uma ou mais funções são atribuídas a esse usuário. As permissões concedidas à função determinam as tabelas que o logon pode acessar e os tipos de operações que o logon pode efetuar. Essa abordagem é usada para criar contas de bancos de dados com menos privilégios que tenham o conjunto mínimo de permissões necessárias para permitir uma funcionalidade legítima e contribuir para a segurança do BD no nível do SQL Server.

A auditoria é uma ajuda vital para a identificação de intrusos e de ataques em andamento, bem como para o diagnóstico de sinais de ataque. É possível configurar um nível mínimo de auditoria para o servidor e elaborar uma combinação de recursos de auditoria do Windows e do SQL Server – por exemplo, através do Enterprise Manager. Isso inclui o modo de autenticação, o nível de auditoria e as contas usadas para executar o serviço do SQL Server. Para isso, deve-se ativar a auditoria de logon do SQL Server e certificar-se de que o serviço do SQL Server é executado utilizando uma conta com menos privilégios.

Finalmente, a capacidade de acessar objetos de banco de dados do SQL Server, como procedimentos armazenados internos, procedimentos armazenados estendidos e tarefas cmdExec, deve ser revisada. Além disso, os bancos de dados de exemplo devem ser excluídos.

3.2 SISTEMAS OPERACIONAIS

Muitas ameaças de segurança existem devido a vulnerabilidades de sistemas operacionais, serviços e aplicativos que são amplamente publicados e conhecidos. Geralmente, quando novas vulnerabilidades são descobertas, o código de ataque é publicado nos BBSs da Internet poucas horas após o primeiro ataque. O patch e a atualização do software do servidor compõem a primeira etapa para a proteção do servidor de banco de dados. Pode haver casos em que a vulnerabilidade exista e não haja patches disponíveis. Nesses casos, deve-se redobrar a atenção aos detalhes de vulnerabilidade para avaliar o risco de ataques e tomar as medidas necessárias.

Os serviços são os pontos de vulnerabilidade preferenciais dos invasores que exploram seus privilégios e recursos para acessar o servidor e, possivelmente, outros computadores. Alguns serviços foram criados para funcionar usando contas com privilégios. Se esses serviços estiverem comprometidos, o invasor poderá efetuar operações privilegiadas. Por padrão, os servidores de banco de dados não precisam de todos os serviços ativados. Ao desativar serviços desnecessários e não utilizados, é possível reduzir de maneira rápida e fácil a área de superfície de ataque.

Uma boa administração das contas de acesso é fundamental para a segurança do BD. Recomenda-se restringir o número de contas do Windows acessíveis pelo servidor ao conjunto necessário de contas de usuário e de serviço, usando contas com menos privilégios e com senhas de alta segurança em todos os casos. Uma conta com menos privilégios, usada para executar o SQL Server, limita os recursos de invasão que compromete o SQL Server e sua capacidade de execução de comandos no sistema operacional.

É possivel utilizar as permissões do sistema de arquivos NTFS para proteger programas, bancos de dados e arquivos de log contra o acesso não autorizado. A combinação de ACLs (Listas de Controle de Acesso) junto com a auditoria do Windows, permite a detecção de atividades suspeitas ou não autorizadas.

Outro item de checagem são os compartilhamentos. Recomenda-se remover todos os compartilhamentos de arquivos desnecessários, incluindo os de administração padrão caso sejam dispensáveis. Proteja quaisquer compartilhamentos restantes com permissões NTFS restritas. Apesar deles não estarem diretamente expostos à Internet, uma estratégia de defesa em camadas com compartilhamentos limitados e seguros reduzirá os riscos se um servidor for comprometido.

Outro ítem de segurança é o modo de autenticação configurado no Registro. Restringir e controlar o acesso ao Registro impede a atualização não autorizada de configurações para, por exemplo, reduzir a segurança no servidor de banco de dados.

3.3 REDE

A nível de Redes, basicamente são dois os aspectos mais relevantes a se observar para a segurança do BD: portas e protocolos. No que se refere às portas, mesmo quando não utilizadas – situação em que ficam fechadas no firewall – é necessário que os servidores subjacentes ao firewall também as bloqueiem ou as restrinjam com base no uso. Para um SQL Server dedicado, basta manter aberta a porta do SQL Server principal e as portas necessárias para autenticação.

Quanto aos protocolos, convém limitar o intervalo de protocolos utilizados pelos computadores clientes para estabelecer conexão com o servidor de banco de dados e verificar se é possível proteger esses protocolos.

4. CONSIDERAÇÕES FINAIS

Durante muito tempo se teve a impressão que uma base de dados era um sistema fechado, dentro de si mesmo, e por conseqüência, seguro. Porém com a difusão de bases de dados, sua popularização e integração de bases diversas, começaram a surgir problemas relativos a erros, integridade e segurança.

Com isto as organizações têm cada vez mais gastos com sistemas que acabam por não gerar informações claras nem concisas, mas que pelo contrário, apresentam falhas de integridade e vulnerabilidades de segurança, resumindo o trabalho dos desenvolvedores e DBA's a "bombeiros" – sempre correndo para apagar os constantes incêndios. Essa

perspectiva, além de carregar implicitamente a idéia errônea de que a T.I. se mantém por emergências e sem planejamento, leva ao risco de que a área seja vista apenas como fonte geradora de gastos e complicações dentro da organização.

Por isso mesmo, é fundamental que o profissional de TI chame para si a responsabilidade e adote um posicionamento pró-ativo no que se refere ao tratamento com Bancos de Dados, conferindo periodicamente seus pontos frágeis e buscando aperfeiçoamento de suas técnicas de proteção. Não só para ter condições de acompanhar as tendências (de linguagens e integração) de tecnologia para manter as empresas atualizadas, mas principalmente para fazê-lo de forma planejada e segura, garantindo às organizações garantias mínimas de sigilo e segurança no arquivamento e troca de dados.

REFERÊNCIAS

CASH JR., J. *et al*. Corporate information systems management: text and cases. Irwin. USA. 1992.

CASTELLS, M. A Sociedade em Rede: a Era da Informação. São Paulo: Paz e Terra. 1999.

CHAPMAN, D.B.; ZWICKY, E.D*, Building Internet Firewalls*, *O'Reilly & Associates*.1995.

DATE, C.J. Introdução a Sistemas de Bancos de Dados. Rio de Janeiro- RJ. Editora Campus. 2000.

GARCIA-MOLINA, H. Implementação de Sistemas de Bancos de Dados. Rio de Janeiro: Campus. 2001.

KENT ,S.; ATKINSON, R. *IP Authentication Header*, RFC 2402, IETF, Novembro 1998.

MACHADO, F. N. R. Banco de Dados: projeto e implementação. São Paulo: Erica. 2004.

MARCOVICTH, J. (Org). Tecnologia da Informação e estratégia empresarial. São Paulo: USP/Futura. 1999.

PORTER, M. Competição = *on competition*: estratégias competitivas essenciais. Rio de Janeiro: Campus. 1999.

SILBERSCHATZ, A. Sistema de Banco de Dados. 3ª ed. São Paulo: Makron Books. 1999.

TARANDACH, I. http://www.securityradio.org, dezembro de 2007.