Segurança de banco de dados (2012).

REBECA SCHAYDEGGER G. QUADROS (Discente - UNES-ES) – *reschaydegger@hotmail.com*

SOLIMAR POCOLI MACHADO (Discente - UNES-ES) – *solimar_machado@hotmail.com*

CHARLES ALTOÉ (Docente - UNES-ES) - *charles_altoe@hotmail.com*

*Resumo**:** Este artigo aborda a questão de segurança em banco de dados, no intuito de contribuir para pesquisa acadêmica, dando ênfase na diferença entre segurança e integridade dos dados e as principais vulnerabilidades do mesmo, apontando ainda algumas medidas de segurança nescessarias.*

Palavra chave: banco de dados; segurança; integridade;vulnerabilidade.

Abstract: This paper addresses the issue of security in the database in order to contribute to academic research, emphasizing the difference between security and data integrity and key vulnerabilities of the same, pointing still some security measures necessaries.

Keyword: database, security, integrity, vulnerability

1. Introdução

O administrador de banco de dados é um profissional necessario à maioria das empresas. Dentre suas copentencias esta uma de suma importacia que é manter o armazenamento dos dados de forma consistente e integrar para que possam ser utilizados sempre que necessario de forma confiavel.

O setor de tecnologia tornou-se peça fundamental no suporte de negócios para as tomadas de decisões estratégicas e contribuindo assim para a sobrevivência da organização. Conforme ressalta Marcovick (1999) estratégias empresariais tecnológicas e de informação tornaram-se sistemas indispensáveis e dependentes para a organização.

Tendo como base a valorização crescente de base de dados bem organizadas e administradas, tivemos uma notória estruturação centralizada de informações que requer uma estrutura no gerenciamento dos dados. O administrador de banco de dados teve o desafio de encontrar modos seguros no tratamento de banco de dados.

Na atual época em que vivemos onde armazenar e transmitir dados são primordiais a segurança dos mesmos, pois a proteção dos dados de modo que a questão de seguranças em SGBD[1] tornou-se o centro das preocupações de TI[2].

Diante disso, pretende-se ressaltar as principais ameaças a bando de dados, como segurança básica de defesa.

[1] SGDB (Sistemas de Gerenciamento de Banco de dados).
[2] TI (tecnologia de informação).

1.1 Conceitos

Banco de Dados: é uma coleção de dados armazenados que se comunicam ou relacionam-se de forma que criem uma linha de raciocínio lógico, são de extrema importância para as empresas. Geralmente existem por muitos anos sem modificações em suas estruturas. Segundo Azevedo (apud ELMASRI (2005)) "Um banco de dados é uma coleção de dados relacionados, que possui algumas propriedades implízcitas".

Segurança: segurança no meio computacional é uma forma de proteção de senhas, logins e etc. Porem se relacionando a banco de dados, podemos dizer que segurança é a proteção e ate mesmo a prevenção para os dados e informações relevantes para uma empresa.

1. Integridade de segurança em sistemas de banco de dados

Os sistemas de gerenciamentos de banco de dados são conhecidos por sua habilidade, rapidez e eficiente a grandes quantidades de dados, outro aspecto determinante para a organização é a integridade de um sistemas de banco de dados e a durabilidade do mesmo. A questão de segurança e integridade começaram a ter destaque, com o crescimento dos bancos de dados a integração ficou mais complexa, propicia a erros tendo um crescimento progressivo.

Em nível de esclarecimento e entendimento, é importante ressaltar a diferença entre conceito de segurança e integridade de dados. Segundo Date (2000) Associando 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 a idéia de proteger o banco de dados, ressaltando no caso da integridade, o foco não esta em invasores externos, e sim restringir acesso a usuários, garantindo assim os que os critérios de permissão de acesso sejam respeitados como foi programado pelo DBA[3].

De acordo com SILBERSCHATZ (1999) "As regras integridade fornecem a garantia de q mudanças feitas no banco de dados por usuários autorizados não resultem em perda da consistência dos dados".

A integridade de dados geralmente são usadas para indicar que os mesmos não podem sofrer alterações de usuários não autorizados. Assim, as regras de integridade protegem o banco de dados de danos acidentais.

2.1 Regras de Integridade.

➔ Afirmação de Claves: conjunto de declarações e modificações autentica restrito, para que não se criem duas entidades (tabelas) com o mesmo nome.

➔ Grupo de relacionamento: limita o relacionamento (N-N, 1-N, 1-1,...) validos vários grupos de entidades (tabelas).

A partir do momento em que planejamos um banco de dados, arquitetamos possíveis maneiras para que aplicações usadas armazenem os documentos corretamente, porem muitos se esquecem de ordenar os níveis de autorização para seus usuários, gerando muitas vezes problemas futuros. Sendo assim foram criados três tipos de integridade diferentes:

[3] DBA (Gerenciador de Banco de dados).

- Integridade de entidade (Tabela): nesse tipo de integridade definimos quais dos atributos serão chaves primarias (PK) e quais serão chaves Únicas (UK), por exemplo, o numero de um CPF é uma chave única (UK), pois ela não pode ser igual à de ninguém não importa o Estado ela sempre será única, só existindo uma para cada cidadão.
- Integridade de domínio: na integridade de domínio podemos definir quais atributos serão nulos (null) e quais podem conter apenas alguns tipos de valores pré-selecionados, por exemplo, Estado civil só poderá aceitar valores do tipo: solteiro, casado, viúvo, divorciado. Podendo apresentar erro caso inserido outros valores que não foram "Programados", o mesmo ocorre com a entidade sexo.
- Integridade referencial: Com a integridade referencial podemos ver referencias das chaves primarias (PK) e únicas (UK), quando esse de chave é referenciado recebem o nome de chave estrangeira (FK), observando que uma chave estrangeira só pode ser criada quando referencia uma chave primaria. Esse tipo de integridade existe para verificar se o dado esta inserido corretamente e se o mesmo (dado) existe como esta sendo referenciado.

Já a segurança no geral, refere-se às regras impostas pelo SGBD que verifica todas as solicitações de acesso. Entretanto a varias vulnerabilidade dos sistemas e ameaças externas, podem resultar no comprometimento do servidor ou na possibilidade de roubo ou destruição dos dados.

É importante ressaltar que a configuração de um SGBD por sua complexidade e importância deve-se ser muito bem administrada tomando algumas precauções especificas. Para melhor entendimento da questão, na figura a seguir mostra uma rotina de uso de uma aplicação em banco de dados, apontando os principais ataques que um sistema pode sofrer.

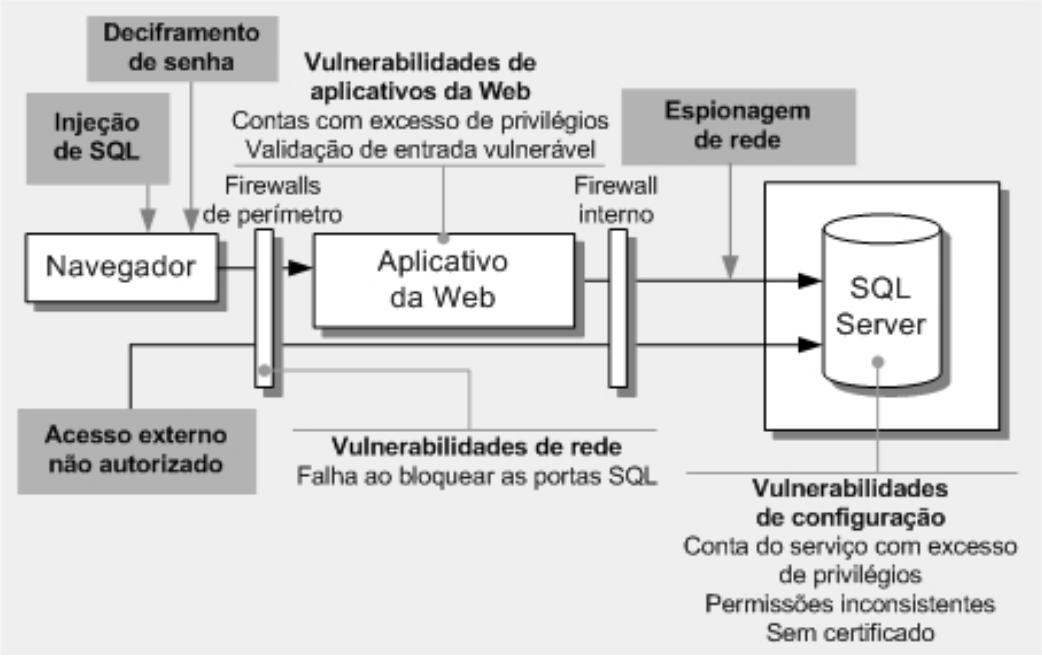

Figura1. Principais ameaças ao servidor de BD segundo a Microsoft (www.microsoft.com).

2.2 Código SQL

Como Date menciona (DATE, 2000:77), a maioria dos produtos de SQL[4] 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[5]. 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 de aplicativo com muitos privilégios ou permissões de baixa segurança que falham ao restringir o logon do aplicativo no banco de dados.

Na tentativa de combater ataques no banco de dados, uma das medidas a se tomar é restringir e corrigir os dados de entradas do aplicativo antes de usá-los em consultas SQL.

Somente consultas SQL segura devem ser usadas para acesso aos dados, uma consulta de comando SQL deve ser construída de forma dinâmica priorizando os procedimentos e seqüência de caracteres. O uso de parâmetro SQL garante que os dados de entrada sejam submetidos a verificações, e que a consulta SQL seja tratada como dado literal, e não como instrução executável no banco de dados.

Outra medida de proteção ao banco de dados é usar o logon do SQL, com permissões restritas, as permissões dos usuários devem ser concedidas somente a procedimento armazenado, não fornecendo acesso direto a entidade.

2.3 Segurança na rede

Na implantação dos aplicativos deve-se atentar para uma separação física entre código de acesso a dados e o servidor de banco de dados. Os dados confidenciais, como dados específicos dos aplicativos ou credenciais de logon do banco de dados devem ser protegidos na rede. Uma das brechas que permitem invasão desses níveis refere-se a canais de comunicação desprotegidos e credenciais não criptografadas, exemplo disso é a autenticação do SQL em vez da autenticação do Windows, ou sem um certificado do servidor onde o SQL esta instalado.

Estalando um certificado de segurança no servidor de banco de dados e usando a autenticação própria do Windows para conecta-se ao servidor de banco de dados é uma das regras para combater tais ameaças de invasão, usando essa medida de segurança resultara na criptografia automática das credenciais do SQL na rede. Para que isso funcione adequadamente é necessário manter uma conexão SSL[6] entre o servidor web e o servidor de banco de dados, protegendo os dados confidenciais.

2.4 Logon não autorizado

Todo usuário ao se logar ao servidor de banco de dados deve ser restrito, para impedir conexões não autorizadas ao banco de dados.

[4] SQL (linguagem de consulta estruturada).
[5] WEB (Rede de alcance mundial).
[6] SSL (Protocolo de chamada de sockets segura).

> 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 as regras de segurança de acesso dos usuários no banco de dados devem-se evitar falhas nas configurações das portas do SQL Serve no firewall, e atentar para a filtragem IPSec. Segundo Azevedo (apud Kent e Atkinson (1998)), o Ipsec[7] 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[8] (Transmition Control Protocol / Internet Protocol). Este se refere a um conjunto de protocolos de comunicação entre computadores em rede.

Os filtros que foram aplicados no IPSec podem ser autorização de um endereço IP[9] ou uma seqüência de IPs de origem/destino específicos, assim como portas específicas de origem/destino.

Tratando-se de acesso ao servidor toda precaução é indispensável uma vez que tantos usuários autenticados sem nome e sem senha estão sujeito a ataque de conexão direta. O exemplo disso um invasor pode estabelecer uma conexão com o banco de dados SQL e obter informações utilizando-se de ferramentas e consultas SQL, ou ainda monitorar as portas para obter informações do servidor.

Para evitar esse tipo de ataque é preciso que as portas do banco de dados não esteja aberta de fora da rede de perímetro, e que dentro da rede o acesso direto seja restrito, isso pode ser feito através dos filtros de IPSec ou TCP/IP.

2.5 Criação de ROLE.

O Gerenciamento de usuários e seus respectivos privilégios aos objetos de banco de dados, dependendo números de objetos e usuários, pode ser tornar uma tarefa árdua para o DBA.

Uma preocupação do DBA em relação ao números de usuários é quando este numero ultrapassa os 10 usuários criados, quando isso acontece o DBA deve tomar cuidados para não liberar permissões (Grants) para os objetos de banco.Uma forma pratica de fazer o processo e a utilização de Roles (papeis).

Role pode ser definida como um “pacote” de privilégios que podem ser associados de forma muito fácil ao usuários de banco.Pode-se criar um Role com permissões totais (administrador) a todos os objetos do banco de dados, sendo assim todos os usuários terão acesso ao papel de administrador.

Sintaxe ***CREATR ROLE atribuição;*** *Na sintexe:* *Atribuição: é o nome da atribuição a ser criada.*

[7] IP sec (Protocolo de interconexao e seguranca).
[8] TCP/IP (Conjunto de protocolos).
[9] IP (Protocolo de interconexão).

Associando todos os usuários a este Role, fica fácil de gerenciar os privilégios (permissões) para um grupo de usuários.

Para um banco de dados com poucos usuários e poucos objetos, esta tarefa é muito simples, usando a linha de comando "CREATE ROLE administrador;" dessa forma você esta criando um role administrador para o banco de dados.

Para atribuir privilégios a este Role, ao invés de atribuir aos usuários, podemos usar as seguintes linhas de comando :

"Grant all on clientes to administrador;"
"Grant all on produtos to administrador;"
"Grant all on estoques to administrador;"

Uma vez que nossa Role administrador já foi criada, e recebeu permissões para os objetos do banco, e hora de associar os usuários a ela, podemos assim usar a linha de comando:

"Grant administrador to Rebeca, Solimar; ".

Assim ficou bem mais simples para atribuir permissões para os objetos do banco.

3 Garantia de senha

Umas das primeiras coisas na tentativa de ataque são tentar quebrar a senha de contas conhecidas, como SA[10]. Nesse quesito, as vulnerabilidades comuns que levam a quebra de senha, geralmente é o uso de senha de baixa segurança ou em branco, e senhas com palavras rotineiras ou comuns.

Alguns programas conhecidos como cracks, que usam dicionários como método de ataque relaciona a tentativas repetidas de palavras existentes para descobrir senhas, aplicando regras combinatórias de forma a prever alterações em palavras que visem a se tornar as senhas mais difíceis.

As tentativas mais comuns de quebra de senhas baseiam-se nesse tipo de ataque de dicionário ou dequitação manual.

Para evitar tais tentativas é de fundamental importância criar senha para contas de logon que atendam a requisitos de complexidade mínima, evitando senhas com palavras comuns.

A utilizar a autenticação do Windows à complexidade da senha poderá ser aplicada pela diretiva de segurança do mesmo.

4 Proteção do SQL Serve

Pode ser complexo proteger banco de dados, especialmente quando se encontra aberto à internet, uma solução interessante é a indução de erros deliberados na programação.

[10] SA (usuário administrador).

Para precaver a proteção de dados, torna-se fundamental o estabelecimento de um checklist para conferencia dos principais elementos do servidor, nesse sentido algumas categorias de configuração (figura 2) recomendadas adquiridas em experiências reais na validação de clientes e em estudos de implantação de segurança.

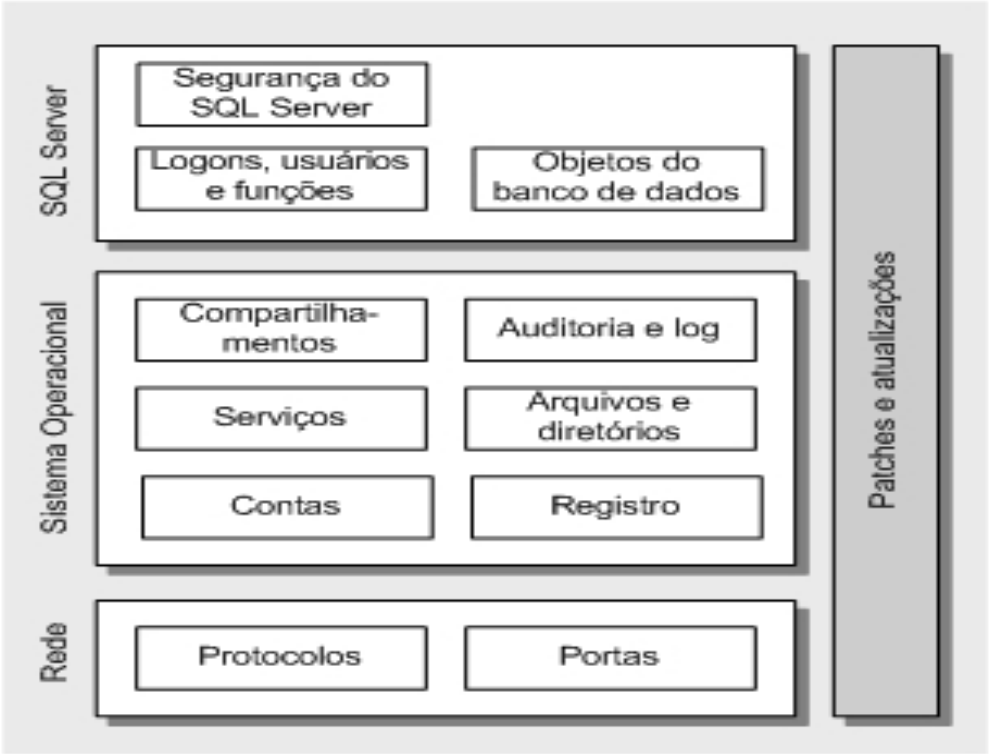

Figura 2. Categorias de segurança do servidor de banco de dados segundo a Microsoft (www.microsoft.com).

4.1 SQL Server.

O acesso dos usuários ao banco de dados é através de logon no servidor, atrais dos atributos e funções de cada usuário, as permissões são determinadas as entidades que podem ser acessadas pelo usuário e os tipos de operações que ele pode executar, as configurações das contas de banco de dados é feita na criação das mesmas, dando privilégios e permissões necessárias de cada logon assim garantindo a segurança de banco de dados.

A monitoração do banco de dados é de vital importância para a identificação e diagnostico de ataques. Pode-se definir o nível de monitoramento do banco de dados através do enterprise manager, ativando a auditoria de logon do SQL através do mesmo você pode monitorar as contas e saber o que o usuário esta executando.

5. Segurança no Computador.

5.1 Sistemas Operacionais.

Muitas ameaças de segurança existem devido a vulnerabilidade de sistemas operacionais, no geral quando são descobertas falhas em sistemas operacionais logo é

publicado na internet a atualização denominada patch que é a primeira etapa para a proteção do banco de dados.

Quando uma vulnerabilidade é descoberta no sistema operacional e não haja Patches disponíveis na internet, deve-se redobrar a atenção aos ataques ao banco de dado. Os ataques de invasão são explorados através das falhas do sistema operacional, alguns serviços foram criados para funcionar usando contas de privilégios, se esses serviços estiverem desatualizados o invasor poderá efetuar operações privilegiadas.

Por padrão, os servidores de banco de dados não necessariamente precissão de todos os serviços ativos, desativando serviços desnecessários assim pode-se reduzir de maneira ágil as chances de um ataque. É recomendado restringir o numero de contas do Windows acessíveis pelo servidor, usando contas com menos privilégios e senhas com alta segurança. As contas com menos privilégios que serão usadas para executar comando no banco de dados, limita os recursos da invasão garantindo a segurança do servidor.

A utilização do sistema de arquivo NTFS[11], ajuda a proteger os programas de banco de dados contra acesso não autorizado. A combinação de ACLs[12] junto com a auditoria do Windows, permite a detectação de atividades suspeitas ou não autorizadas. Vale ressaltar como ponto importante são os compartilhamentos. É recomendável remover todos os compartilhamentos de arquivos desnecessários, para proteger os compartilhamentos restantes podem-se usar as permissões NTFS restritas, apesar dos mesmos não estarem diretamente expostos a internet, uma estratégia de defesa em camadas com compartilhamentos limitados, reduzira os riscos de invasão do servidor. Outro item de segurança é o modo de autenticação configurado no registro, restringir e controlar o acesso ao registro impossibilita a atualização não autorizada de configurações, como por exemplo, reduzir a segurança do servidor de banco de dados.

5.2 **Seguranças via rede.**

Basicamente nível de redes os aspectos mais relevantes são portas e protocolos. As portas mesmo quando não utilizadas são monitoradas através do firewall, que as bloqueiam e restringem o seu uso. Quanto aos protocolos a melhor opção é limitar o intervalo de protocolos utilizados pelos computadores para estabelecer conexão com o banco de dados.

Considerações Finais.

Com o alto crescimento e utilização de banco de dados começou a surgir problemas relativos a erros, integridade, segurança, com isso as organizações vêm investindo cada vez mais pesado em sistemas que possam gerar agilidade, segurança e integridade para os banco de dados. É de vital importância que o profissional de TI tenha total responsabilidade, adotando um posicionamento que se refere ao tratamento com banco de dados, verificando diariamente os pontos frágeis e buscando aperfeiçoamento de suas técnicas de proteção para maior segurança da empresa.

[11] NTFS (new technology file system).
[12] ACLs (Lista de controde de acesso).

Referências

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

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

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

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

MACHADO, F. ABREU, Mauricio. **Projeto de Banco de Dados.** 5° edição, São Paulo: Erica, 2000.

SETZER, Valdemar S. **Banco de dados.** 3° Edição, São Paulo: Edgard Blucher, 1999.

SILBERSCHATZ Abraham; KORTH Henry, SUDARSHAN S. **Sistemas de Banco de Dados.** 5° edição, São Paulo: Campos, 2006.

ROB, Peter. **Sistemas de banco de dados: projetos, implementação e administração.** 8° Edição, São Paulo,Cengage Learning, 2010.

SMITH, Ronaldo. **SQL Serve 7**. 1° Edição, Rio de Janeiro: Brasport, 1999.

ELMASRI, Ramez. **Sistemas de banco de dados**. 6° Edição, São Paulo: Pearson Addson Weslet, 2001.

ALTOÉ, Charles. **Banco de dados gerenciamento de usuários**. Espírito Santo, 2012. Nove (9) diapositivos.

Microsoft knowledge base. São Paulo 2012. Disponível em: <http://www.spport.microsoft.com >. Acesso em 21 abril 2012.