Atividade BD – Defesa em profundidade

Alunos

Luiz Felipe

Pedro Luiz

Tomaz Barrantes

Defesa em Profundidade para Alcançar Segurança de banco de dados “inquebrável” - Artigo

1. Na MDACA qual é a primeira camada de segurança?

Controle de Acesso, as contas e privilégios de usuário do banco de dados são considerados como primeira camada do MDACA..

1. Qual a principal vantagem de administrar um banco de dados atribuindo privilégios através de papéis?

Um papel agrupa vários privilégios, portanto podem simplificar a administração de segurança em bancos de dados com grande número de usuários ou com um sistema de segurança complexo

1. Explique, segundo o artigo, como uma STORED PROCEDURE pode ser usada para restringir os privilégios de um usuário.

Uma maneira de restringir os privilégios é através do encapsulamento de privilégios em STORE PROCEDURES, ou seja o usuário somente executaria uma função através da STORE PROCEDURE. Por exemplo, um usuário de modo geral não teria o privilégio de INSERT, ou seja atualizar uma tabela, entranto ao executar uma STORE PROCEDURE, este privilégio seria dado somente durante a execução da STORE PROCEDURE, desta forma formando mais uma camada de Segurança.

1. Descreva o que é o CONROLE DE ACESSO POR LINHA do banco de dados, e cite um exemplo de como pode ser implementado por um Application Servide Provider.

O controle de acesso no nível de linha (também conhecido como granular controle de acesso no Oracle9i) permite construir aplicativos e aplicar políticas de segurança em um nível de granularidade de linha. Pode-se usá-lo, para restringir um cliente que está acessando um banco de dados para ver apenas a conta do cliente, um médico para ver apenas os registros dos próprios pacientes do médico, ou um gerente para ver apenas os registros de funcionários que trabalham para o Gerente. Para isso é necessário criar políticas de segurança anexadas às tabelas de banco de dados e exibições para a aplicação dada.

1. O que significa o termo "One Big Application User"?

As aplicações de pacotes comerciais, especialmente aplicações Web não são diretamente usuários da base de dados, para estas aplicações se autenticam a uma aplicação e se conectam ao banco como um simples usuário, originando o que se chama de “One Big Customer”, portanto muitas funcionalidades da base não podem ser utilizadas, e portanto funções da MDACA (Multi-layer Database Access Control Architecture) como Controle de Acesso e Roles não podem ser utilizados.

Isto leva a Segurança ser implementada pelas aplicações, tornando a solução mais Cara.

1. Qual a recomendação para substituir o uso do "One Big Application User"?

Implementar o login único em que as organizações centralizam as informações do usuário e gerenciamento em um diretório baseado em LDAP

1. Por que se afirma no artigo que a criptografia limita os poderes do administrador do banco de dados?

As contas administrativas começam como anônimas e todo poderoso, permitindo que os administradores acessem informações que eles querem sem serem responsabilizados.

A criptografia impede o administrador para visualizar os dados criptografados se somente o proprietário detém chaves de criptografia.

1. Quais são dos dois pontos de atenção quando se adota o uso de criptografia dos dados?

• A criptografia não resolve problemas de controle de acesso – eles são responsáveis pelas outras camadas do MDACA.

• Criptografar tudo não torna os dados seguros - dados criptografados podem ser excluídos ou modificados. É importante manter os backups apropriados para que, se alguém exclui ou altera os dados criptografados, eles podem ser restaurado.

1. Explique os conceitos de *Criptografia de “data-in-motion” e Criptografia de “data-at-rest”*

Criptografia de “data-in-motion” ocultam informações que atravessam a rede a partir do banco de dados para o cliente ou do cliente para o banco de dados. "Data-in-motion" inclui tráfego que passa pela sua rede local, pela Internet ou até mesmo através de uma rede sem fio.

Por exemplo, SSL (Secure Sockets Layer) e Kerberos criptografia de rede são integrados ao Sybase ASE 12. Além de proteger a confidencialidade de informações em trânsito, cada solução autentica um ASE identidade do servidor. SSL usa criptografia de chave pública e autentica a identidade de um banco de dados por meio de um certificado digital, enquanto o Kerberos autentica mutuamente um banco de dados e um usuário quando o usuário faz logon.

A criptografia de “data-at-rest” envolve a transformação, informações armazenadas no banco de dados em um formulário para que seja legível por pessoas autorizadas. Tanto o Oracle9i quanto o Sybase O ASE 12 suporta criptografia de “data-at-rest”.

Atividade questões de Segurança de Banco de Dados - Segurança em Profundidade

1. Por que o a segurança do banco de dados deve estar integrada as demais iniciativas de

segurança do bd?

**Por que fazer essa integração pode garantir mais segurança para o banco de dados, pode minimizar o riscos de falhas e erros no banco de dados e esse tipo de segurança pode estar alinhado ao negocio da empresa garantindo mais segurança e proteção ao banco e aos dados sensíveis da empresa. Fazer esse tipo de integração da visão mais ampla do negocio e permite alinhas o banco juntos as ferramentas de segurança que haverá na empresa.**

2. Por que se diz que é desbalanceado as forças de quem ataca e de quem defende?

**Por que podem existir algumas falhas e exploração de vulnerabilidades de ferramentas que são conhecidas pelo atacante não são conhecidas pelo defensor ou implementada na segurança da aplicação. Pode haver alguns desbalanceamento devido a falta de investimento em ferramentas ou falta de mão de obra capacitada para defender mais esse tipo ocorrer de quem ataca e defende.**

**O que pode ser balanceado é ter profissionais que conhecem a ferramenta, conheçam sobre boas praticas de segurança e que saiba proporcionar essa pratica na segurança de aplicações e do banco de dados e também a necessidades de profissionais que saibam trabalhar toda segurança e defesa da melhor forma.**

3. O que permite que ocorra um ataque de dia zero?

**Podem ocorrer devido a falta de atualização de patchs de segurança ou por falta de informações e explorações de novas falhas que são descobertas e não são notificadas ou noticiadas na comunidade. Pode ser implementado ou explorados falhas de ferramentas que estão instalada na empresa. E explorada algumas configurações de ferramentas que precisam ser atualizadas ou alteradas conforme a utilização. Esse tipo de ataque pode ser feito de forma muita rápida onde não é conhecida de usuário ou administradores de aplicação.**

4. Exemplifique o uso de várias camadas de segurança para a defesa em profundidade

**Alguns exemplos de camadas de seguranças para uma boa defesa, a implementação de firewall na rede e uma boa configuração de proxy, um implementação de boas ferramentas de IPS e IDS para proteção de perímetro de rede, Implementar segurança no código de desenvolvimento e também boas praticas de desenvolvimento seguro, pode ser implementado uma boa Ferramenta de VPN e que pode ser agregada a uma criptografia do banco e a implementação de boas práticas de segurança em controle de acesso e autenticação de aplicações e do próprio banco de dados**

5. Qual a importância da política de segurança corporativa para a segurança da informação em profundidade?

**A política de segurança é importante devido a necessidade de implementação de boas práticas de técnicas de segurança para aplicação e para ativos e ferramentas que a empresa irá proporcionar.**

**Ela existirá para que se tenha regras para os administradores de sistema e profissionais da empresa tenha noção da como poderá garantir a melhor configuração ou melhor ferramenta de proteção para determinado ativo. Isso garante que se diminua os riscos de falhas ou problemas na aplicação e no setor do negócio. E irá proporcionar que se tenha mais profundidade na hora de garantir a segurança da aplicação e do banco de dados, a política pode ser criada para ditar as praticas de backup e criação e liberação de acessos, poderá também exigir mais responsabilidade na hora de uso das ferramentas que empresa fornece e quanto mais profundo for na aplicação de segurança da informação melhor será garantia evitar perdas e falhas na hora de agregar a ferramenta ao negócio.**

6. Quais são os principais métodos de autenticação?

**OS principais métodos são senhas, PKI, SSL, certificados digitais, tokens, cartões inteligentes e biometria**

7. Single sing on é uma realidade no mercado?

**Sim pois Single ON traz o conceito de autenticação dupla onde permite gerenciar qual a identidade de acesso do usuário, e se é o próprio usuário que esta acessando a aplicação, esse tipo de ferramenta permite implementar mais segurança e informações nos logs de aplicações e permite mostrar qual ponto de acesso foi utilizado para o acesso**

8. Diferencie Firewals, vpns e sistemas de intrusão e prevenção

**Firewall são as ferramentas de segurança de perímetro de rede que protegem os acessos n internet e extranets e podem proteger alguns domínios de rede.**

**As VPNS são as redes virtuais privadas e onde permite criar os perímetros de gestão da rede e melhor o acesso da rede, onde permite implementar os grupos de equipamento que terão o acesso e como será feita a gestão do domínio da rede**

**O sistema de intrusão e prevenção são os sistema que monitoram junto com firewall a segurança da rede e pode ser criar mecanismos da alerta e proteção da rede.**

9. Como ser proativo para tornar mais segura a sua infraestrutura?

**Ser proativo pode garantir mais conhecimentos da rede e infraestrutura e permite garantir conhecer melhor as ferramentas e evita que haja falhas ou riscos na rede, o administrador sendo desta forma permite que a infraestrutura esteja segura e mais protegidas contra o ataques de zero day, que protege e garante mais proteção para rede.**

10. Pesquise e relacione 3 produtos de Gestão da Segurança da Informação

**Os produtos são firewall da cisco ou um web firewall que permite gerenciar o acesso nas aplicações e garantir mais segurança.**

**As ferramentas de checkpoint e antivírus da Symantec ou KArpersky que garantem que a empresa esteja com o ambiente protegido e seguro contra vírus.**

**E um terceiro produto é as ferramentas de monitoramento como Zabix ou Squid que monitoram e protegem a rede**

11. Cite os tipos de antivírus encontrados no mercado

**A diversos antivírus no mercado por exemplo scans online, sistema de busca e escudos em tempo real, software antivírus de rede, antivírus em gateways de e-mail, antivírus de desktop, antivírus de aplicações, antivírus de navegadores web entre outros.**

12. Explique com suas palavras por que se diz que o modelo de aplicação web é inerentemente inseguro.

**Podemos compreender que o modelo de aplicação web ele é inseguro devido o processamento ser feito todo no servidor, ou seja, no back-end e no prisma do navegador somente é apresentada uma página, e é feita uma coleta de informações do usuário, e a comunicação desses dados de volta para o servidor. Essa comunicação é realizada através de uma solicitação HTTP, e de uma perspectiva de cliente-servidor, o modelo é stateless, ou seja, as solicitações de entrada não estão relacionadas com quaisquer outras solicitações de entrada, assim é fácil alterar as requisições e respostas trocadas entre o servidor e o cliente, a partir de qualquer uma das páginas que compõem o aplicativo. Deixando uma grande brecha a ser explorada por hackers.**

13. Descreva onde está a maior oportunidade de melhoria para se ter um aplicativo mais seguro

**Atualmente foca-se na oportunidade de melhoria no desenvolvimento da aplicação, temos o recente surgimento do DevSecOps que é um conceito que mescla a segurança da informação junto com o desenvolvimento e testes antes mesmo da aplicação estar pronta, com isso a empresa economiza e muito, ao invés de lançar um software sem se atentar com a segurança e fazendo a correção de acordo com as falhas que vão surgindo o que pode acarretar insatisfação e grandes prejuízo dependendo da falha.**

14. Descreva o processo de gerenciamento de vulnerabilidade

**O processo inclui várias tecnologias (alguns dos quais já foram discutidas) e um conjunto de processos que fornecem a cola para essas tecnologias. Vide imagem abaixo.**



15. Descreva a taxonomia de vulnerabilidades criada pelo Gartner Group

**O Gartner Group divide essa taxonomia em dois grupos, o primeiro sendo defeito de software e o segundo erro de configuração, dentro desses grupos ele faz subdivisões, sendo a do primeiro grupo falha de software a falhas no projeto como um primeiro tópico dessa categoria e erros de codificação o segundo tópico dessa categoria. Já no segundo grupo o primeiro tópico é sobre serviços desnecessários (e perigosos) e o segundo tópico é envolto de erros na administração de acessos.**

16. Qual a origem dos maiores incidentes de vulnerabilidades?

**São os erros de configuração que representam 65% das vulnerabilidades.**

17. Por que se diz que erros na administração de acessos podem desmoronar o modelo de segurança?

**Os erros na configuração do controle de acesso, podem ser desastrosos para a segurança. Principalmente devido a exploração de tais erros normalmente não pode ser facilmente detectado pelo monitoramento, pois do ponto de vista externo, o acesso parece correto**

18. Pesquise 3 produtos do tipo scanner de vulnerabilidade

**Há vários tipos de scanners, incluindo avaliações baseadas em host, em rede, no alvo, entre outros.**

19. Quais os principais tipos de scanners de vulnerabilidades?

**Dentre os diversos existentes os scanners baseados em aplicativos, scanners orientado a objetivo, scanners “Host-Based”, e o scanners baseados em rede e os scanners web estão entre os principais do mercado.**

.

20. Por que se diz que o gerenciamento de patches não é tão simples quanto parece?

**Porque dentro de uma empresa pode incluir muitos sistemas, mas o rastreamento do que ela tem instalado, onde, com qual patches, e quem os instalou é um grande desafio e muito difícil.**

**Fora que além de saber o que está instalado, é preciso controlar o que você necessita instalar e as vulnerabilidades são descobertas o tempo todo, e os vendedores liberaram continuamente patches dificultando ainda mais esse processo de gerenciamento.**

21. Qual a importância de se fazer um planejamento para a execução de patches

**Fazer esse tipo de planejamento pode evitar falhas e paralizações involuntárias por falhas de infraestrutura e equipamento e importante pois pode planejar quando será feita e quando será implementada para que não haja problemas na implementações.**