9) Segurança no SGBD

9.1) Segurança Física

9.1.1) Segurança do Hardware

Atualmente, segurança para servidores de bancos de dados não é uma opção mas um requisito, especialmente se o servidor estiver numa rede. Conhecer como permitir aos clientes chegarem ao SGBD e como evitar que outros não cheguem é uma tarefa importante para o DBA.

É importante que o hardware onde encontra-se o servidor do PostgreSQL, seja um hardware além de robusto fisicamente, seguro. Para isso diversos cuidados devem ser tomados:

- Fontes redundantes
- RAID com HDs

  Muitos outros cuidados semelhantes, em especial que a origem do hardware seja confiável e tenha uma boa garantia.

Importante uma leitura do **PostgreSQL Hardware Performance Tuning:**

http://www.postgresql.org/files/documentation/books/aw_pgsql/hw_performance/

Traduzido: http://www.vivaolinux.com.br/artigos/impressora.php?codigo=5930

9.1.2) Segurança no Acesso Físico ao Servidor

Sem garantir segurança física ao servidor de nada vai adiantar os cuidados com a administração do mesmo, com usuários, senhas, etc. Primeiro garantir boa segurança no hardware, depois garantir que somente pessoal de confiança tenha acesso ao servidor. Finalmente a segurança lógica.

A segurança física, de acesso ao servidor, deve ser levada em conta e receber a devida atenção para que as informações possam de fato ser protegidas.

Por padrão, o PostgreSQL é instalado no Windows em: C:\Program Files\PostgreSQL\8.3 e no

Linux, quando através dos fontes em: /usr/local/pgsql

Para saber o nome dos arquivos dos respectivos bancos de dados podemos usa a consulta:

```
select oid, datname from pg_database;
```

Uma forma de esconder um pouco alguns bancos é criando um Tablespace e os armazenando em outro diretório. Vide capítulo 2 do módulo 2.

Em termos de Sistema Operacional, tudo indica que um Linux seja mais seguro para um servidor do SGBD PostgreSQL, devido ao seu sistema de permissões e controle de usuários, que é mais exigente que o de um Windows. Sem contar que existem indícios de ser um ambiente para maior desempenho.

A Segurança da Informação Pessoal e Corporativa

O conceito de segurança da informação não está ligado somente à computadores e seus sistemas, este é um termo muito mais amplo utilizado para dar a idéia de segurança de dados pessoais ou corporativos.

O termo sempre é associado à segurança de informações digitais, mas devemos nos lembrar que a informação pode estar em qualquer mídia, um cd-rom, um pendrive, uma folha de papel, um bloco de notas, uma agenda…

Imagine que você tem uma agenda, dessas de papel (lembra que isso existe?), e nesta agenda você tem todos os seus dados pessoas, compromissos, telefones de amigos e familiares, contatos profissionais, informações bancárias e etc. Agora imagine que você perde essa agenda… O que fazer? Toda a sua vida está nela, será muito fácil alguém se passar por você de posse te todas essas informações.

Da mesma forma funcionam seus dados digitais, praticamente todos que usam computadores mantém algum tipo de dado pessoal armazenado nele. E a segurança disso? A diferença da a boa e velha agenda de papel é que os computadores podem ser acessados à distância, sem você saber. Porque é mais fácil conseguir informações no meio digital? Ora, encontrar uma agenda na rua não é algo tão comum, mas encontrar sistemas de informação sem proteção ou com proteção fraca é. Vamos pegar como exemplo uma rede corporativa com, por exemplo, um sistema acessado por meio de autenticação com senha. Esse sistema foi projetado e concebido com a idéia de ser seguro, ele usa conexão criptografada e ainda pede para a pessoa digitar algo aleatório exibido em uma imagem (Captcha) para evitar ataques de força bruta. Certo, até aqui temos um bom sistema, um sistema seguro e com uma bela muralha na frente. Qual seria o principal ponto fraco desse sistema supondo que não há bugs ou falhas exploráveis na autenticação dos usuários? Quer uma dica? Começa com ‘Usu’ e termina com ‘ários’. É isso mesmo, de que adianta o alto investimento em um sistema seguro se o usuário anota a senha em um bloco de notas e o deixa em cima da mesa à vista de qualquer um? O que acontece quando o usuário usa como senha o próprio nome? Ou palavras simples? Ou mesmo seqüências de teclas no teclado como ‘qwerty’ e ‘asdfg’? Ou mesmo o famoso ‘123′?

Pronto a segurança foi para o espaço, pouco adiantou investir alto no desenvolvimento de algo seguro.

Todas as empresas, usando computadores ou não, deveriam ter um mínimo de preocupação com a segurança de informações. Estabelecer regras de comportamento para os funcionários, treiná-los para seguir essas regras, monitorar constantemente se estão seguindo tudo de conforme definido.

A falta de regras e treinamento pode levar os usuários a ter um 'comportamento de risco'.

Políticas de boa utilização de dados e de segurança devem fazer parte da vida de todos, não apenas de grandes corporações, as micro e pequenas empresas estão sujeitas a ataques também, aliás os usuários domésticos correm riscos igualmente!

É claro que o pensamento 'quem vai querer me invadir?' existe. Afinal de contas quem vai querer invadir o meu pc? Eu não tenho informações de grande valor mesmo. É, mas com várias pequenas informações e muitos 'bots' se pode fazer muita coisa ilegal. Imagine a Polícia Federal chegando em sua casa com a acusação de que centenas de e-mails SPAM partem da sua conexão diariamente. Isso sim é uma situação desagradável, como provar que não é você o responsável se o programa que envia as mensagens está instalado no seu computador e disparando o tempo todo? Pois é meu amigo, ou você acha que para esse tipo de coisa os cybercriminosos invadem apenas os servidores da Nasa?

Como você pode proteger suas informações e seu computador de possíveis ataques?
- Mantenha um bom firewall ativo
Ele bloqueia conexões indesejadas.
- Não clique em links recebidos por e-mail
Mesmo que você tenha, supostamente, ganhado $ 1mi.
- Não divulgue seu e-mail de forma irresponsável
Bots de rede varem sites em busca de e-mails
- Tente não seguir as malditas correntes de e-mail
Você sabia que seu IP vai no e-mail enviado?
- Nunca responda e-mails de desconhecidos
- Não aceite programas que lhe enviam por e-mail ou softwares de mensagens instantâneas
Para isso vá ao site do desenvolvedor e baixe o software ou compre
- Não utilize software pirata
Eles vem com cracks que, além de quebrar a segurança do programa, contém vírus, spyware e malware em geral.
- Não utilize senhas simples!

Entrar no e-mail de alguém que deixa a senha 'qwerty' não pode nem ser considerado crime, já que essa senha e senha nenhuma nenhuma senha são praticamente equivalentes.
- Mantenha um bom anti-vírus
Sim, esse é um dos fatores principais (Ainda mais se você usa o sistema número um em quantidade de vírus). Preciso dizer que anti-vírus 'crackeado' é inútil?
- Proteja seu computador com senha
O atacante pode ser uma visita que liga o pc e pega as informações.
- Não acesse o site do banco em lan-houses!

Nestes lugares podem estar ativos os chamados Keyloggers que guardam todas as teclas digitadas. Ou seja, a grande sacada é agir com bom senso e evitar armadilhas.

Nunca dê seus dados à pessoas que ligam oferecendo serviços e produtos ou mesmo dizendo ser do banco, da Receita Federal, etc… Sempre que precisa ou desconfiar de algo vá ao banco ou ligue, vá ao posto de atendimento da Receita, mas não acredite em ligações!

A segurança da informação é algo que é praticamente impossível de ser 100% efetiva, sempre existem falhas humanas, falhas nos softwares, falhas nos cadeados, agendas se perdem…
Mas agindo com bom senso, guardando bem os dados pessoais, protegendo as informações nos computadores e identificando possíveis golpes é possível tornar seu dia-a-dia bem melhor.
Não pense que ninguém quer suas informações porque elas não valem nada, elas valem sim, mas eu tenho certeza que para você e sua empresa elas não têm preço.
http://infog.casoft.info/?p=32

9.2) Segurança Lógica do SGBD

Jamais aconselharia deixar dessa maneira para um banco em produção. Com isso o usuário postgres poderia ter acesso (mesmo que com senha) de qualquer máquina da rede. Aconselho a permitir conexões com o usuário postgres apenas para os endereços 127.0.0.1/32 e o ip do servidor/32. E não use o usuário postgres como usuário de conexão em nenhum dos casos. Tenha um usuário apenas com os GRANTs necessários para não deixar a segurança da sua base de dados vulnerável.

Fernando Brombatti na lista pgbr-geral.

Cada aplicação deve ter um usuário com acesso apenas ao necessário para usar a aplicação.

As configurações default do postgresql rejeitam toda conexão de outros computadores e usam

a autenticação do tipo ident para gerenciar o acesso de usuários com mesmo nome no sistema operacional (isso em Linux/UNIX/BSD, não no Windows).

As versões atuais também suportam autenticação tipo LDAP.

Segurança no Sistema de Arquivos

Por default quando instalamos o PostgreSQL no Linux através dos fontes ele é instalado em:

/usr/local/pgsql

No Windows uma instalação com o instalador ele fica em:

C:\Arquivos de Programas\PostgreSQL

Os programas executáveis, como o pg_dump, o psql e outros ficam num subdiretório bin desse diretório de instalação.

Os bancos, logs e outros arquivos ficam no subdiretório data. Dentro desse sibdiretório data ficam alguns diretórios importantes como o base (que abriga os bacos de dados), o global (que guarda informações de todos os bancos) e o pg_xlog (guarda os logs de transações).

Os bancos que ficam no diretório data/base são gravados com números dos OIDs. Para saber que banco corresponde aos OIDs podemos usar uma consulta à tabela de sistema pg_database:

```
dnocs=# select oid, datname from pg_database;
  oid  |     datname
-------+------------------
 10819 | postgres
 16400 | template_postgis
 16816 | iniciante
 16821 | dnocs
     1 | template1
 10818 | template0
 16835 | biblioteca
(7 rows)
```

Uma boa prática é monitorar as informações detalhadas sobre os arquivos e diretórios do PostgreSQL: permissões, data de criação e modificação, dono, etc.

Lembrando que no Linux a permissão de execução em diretórios permite listar o diretório e o acesso ao diretório.

Conexões Remotas

Também devemos tomar precauções ao conectar remotamente ao servidor, usando conexões seguras como SSH.

Veja outras recomendações sobre Conexões TCP/IP seguras por túneis SSH em:

http://pgdocptbr.sourceforge.net/pg80/ssh-tunnels.html

E Conexões TCP/IP seguras com SSL em:

http://pgdocptbr.sourceforge.net/pg80/ssl-tcp.html

9.2.1) Segurança relativa aos usuários

Em relação aos usuários, grupos e privilégios, já vimos na aula 4: 4) Administração de Grupos, Usuários e Privilégios.

Esta segurança é interna do SGBD. Mas antes que chegue ao SGBD deve passar por uma barreira de segurança chamada Firewall, depois de passar pelo Firewall deve ainda passar pelos scripts postgresql.conf, pelo pg_hba.conf e. pg_ident.conf (caso esteja num Linux).

Firewall – esta é a mais básica barreira de segurança de um servidor que encontra-se numa rede. Ele nos permite filtrar que clientes irão passar pelo firewall para que aplicações. Enquanto podemos ter um único firewall protegendo toda uma rede, também podemos ter um firewall protegendo um único servidor. Quando habilitamos um firewall, por default, está tudo bloqueado. A partir daí precisamos desbloquear cada cliente que deve ter acesso.

postgresql.conf - Este é o primeiro script que o cliente remoto encontra quando pretende conectar com o servidor do PostgreSQL. O acesso remoto e muitas configurações importantes começas neste script. Para que clientes remotos tenham acesso precisamos alterar a configuração padrão de localhost para *:

listen_addresses = '*'

pg_hba.conf - O próximo passo é a configuração do pg_hba.conf, que define que usuários podem conectar a que bancos, usando que IP ou rede com respectivas máscaras e com que sistema de autenticação. Cada linha define uma individual regra de acesso. Somente terá acesso se satisfazer a todas as colunas.

O pg_hba.conf permite linhas de três tipos: comentátios, em branco e registros (linhas válidas ao final). Os registros podem ser separados por tabulação ou espaços. Espaços no início e ao final são ignorados. Um registro obrigatoriamente deve ser contido em uma única linha.

As colunas de cada linha do script são:
conxão-tipo banco usuário end_rede método-login opções

Exemplo:

hostssl	all	all	10.0.1.0/28	password
host	teste	joao	192.168.120.5	md5
host	teste2	joao	192.168.120.5	md5
host	teste3	all	10.0.2.0/28	md5

O tipo de conexão pode ser:
local – conexão local ao SGBD,
host – conexão permitida somente quando existe o suporte à conexões tipo TCP/IP.
Hostssl – deve estar habilitado o suporte a SSL.

Para testar uma conexão remota podemos usar um cliente como o psql:

psql -h 10.0.1.33 teste joao

Habilitando SSL no PostgreSQL

A instalação for Windows já suporta SSL por default. No Linux devemos verificar ou habilitar.

Habilitar no postgresql.conf:

ssl = on

Após restartar o servidor ele estará escutado por conexões normais (TCP) e conexões SSL (SSL TCP) na mesma porta. Logo que conecta com suporte a SSL o PostgreSQL procura a chave de criptografia e os arquivos do certificado no diretório 'data' e não iniciará até que encontre os mesmos. Vide capítulo 3 do Livro "PostgreSQL 8 for Windows".

Obs.: Nunca use o tipo de autenticação **trust** em redes que não ofereçam uma boa segurança.

O tipo de autenticação **ident** deixa a cargo do cliente a segurança.

Antes de efetuar alterações no tipo de autenticação do pg_hba.conf, por exemplo, para md5, conceda senha ou as altere para todos os usuários, como a seguir:

CREATE ROLE usuario WITH ENCRYPTED PASSWORD 'senha';

ALTER ROLE usuario WITH ENCRYPTED PASSWORD 'senha';

Obs.: Se a senha for em texto claro, do tipo **password**, não use a palavra ENCRYPTED

Após isso altere o pg_hba.conf e restart o servidor.

Rejeitando Conexões

Um dos métodos de autenticação é o **reject**, que pode ser aplicado em caso de suspeita ou certeza de conexão não desejada.

Exemplo:

```
host all      192.168.0.15      255.255.255.255 reject
```

Monitorando Usuários

Através do PGAdmin podemos monitorar muito bem todos os usuários e suas ações.

Após conectar clique em Ferramentas – Status do Servidor.

Aí podemos monitorar o PID, usuário, banco, IP, início da conexão, consultas, etc.

Como também os bloqueios, as transações e o arquivo de Log. Até rotacionar o arquivo de Log,

caso necessário e caso o usuário conectado tenha este privilégio.

Referência: Capítulo 10 do Livro PostgreSQL 8 for Windows.

9.2.2) Segurança do projeto dos bancos dados e seus objetos e consultas e código SQL

Esta parte diz respeito ao código SQL das consultas, que deve comtemplar pelo menos as 3 formas normais, sempre usar chaves primárias nas tabelas, índices em campos muito consultados na cláusula WHERE e boas constraints que venham a melhorar a segurança das consultas.

Também vale lembrar que é útil o uso de VIEWS, de funções e procedures.

Usuários autorizados podem se aproveitar da estrutura dos objetos do SGBD para ter acesso ao que não devia.

9.2.3) Segurança dos aplicativos (senhas, usuários, etc)

Este tópico deve fazer parte da política de segurança da empresa/instituição para suas informações.

Aplicativos devem usar senhas fortes e renovar as mesmas com certa periodicidade.

Veja alguns bons artigos sobre segurança com senhas:

http://www.microsoft.com/brasil/technet/Colunas/DiogoHenrique/SenhasAltaSeguranca2.mspx

Recomendações e Procedimentos de Segurança :

http://www2.iq.usp.br/sti/index.dhtml?pagina=754&chave=89N

Recomendações para Política de Senhas:

http://www.brasilacademico.com/maxpt/article_read.asp?id=190&ARTICLE_TITLE=Recomenda%E7%F5es+para+Pol%EDtica+de+Senhas&CATEG_Title=Dicas%3A+Seguran%E7a

Desafios da Segurança de Informação

Autor: Anderson de Sousa Pereira <link.twister at gmail.com>

Desafios

O maior desafio para as empresas é manter a segurança de seus dados, e quando falamos em segurança de dados não devemos ter o luxo de ignorar qualquer tipo de risco que possa comprometer a integridade dos mesmos. E esses riscos envolvem corrompimentos de dados, perda, roubo, entre outros fatores... Isso pode ser ocasionado devido a fenômenos naturais como, furacões, inundações, terremotos... E também podem ocorrer devido á uma má administração.

O maior perigo para uma empresa é ter a falsa sensação de segurança. Afinal, pior do que não se preocupar com invasões, ataques, vírus, tragédias entre outras ameaças é confiar cegamente em uma estrutura que não esteja preparada para impedir o surgimento de problemas.

Por isso, não devemos confiar apenas em software, ou hardware. Quando falamos em segurança da

informação, é necessário considerar quatro obstáculos que têm a mesma importância: a natureza, as pessoas, a tecnologia e os processos.

Não adianta investir apenas em um deles e deixar os outros de lado, eles devem ter a mesma atenção. E os quatro devem estar intimamente ligados, afinal um necessita do outro. Quanto a tecnologia, natureza e processos até que não é um desafio tão gritante, o maior desafio mesmo são as pessoas.

Quanto a natureza, nós podemos nos prevenir com um estudo do local onde a empresa será implantada e mantendo copias dos dados em outros locais, afinal até alguns anos atrás aqui no Brasil eu não me preocuparia com furacões e terremotos, mas ultimamente com o aquecimento global tudo é possível, só do ano de 2007 até hoje já tiveram vários tremores em algumas cidades do nosso país, claro que isso é só a ponta do iceberg...

Quanto à tecnologia e processos, desde que sejam bem administrados e usados corretamente se tornam ferramentas essenciais para o crescimento e evolução do negócio. Parece fácil, mas embora a teoria seja lógica, fazer com que sejam bem implantados é uma difícil e árdua missão. Afinal, é aí que entram as pessoas, cada um usando a tecnologia a seu favor e muitas vezes para fazer um mal uso. E quando eu falo de pessoas eu estou me referindo aos usuários (meros mortais) que dedicam suas vidas à atormentar o CSO (Chefe...xD). Grande parte dos incidentes de segurança contam com o apoio, intencional ou não, do inimigo interno. As pessoas estão em toda a parte da empresa.

Os cuidados básicos com as atitudes das pessoas, muitas vezes são esquecidos ou ignorados. Encontrar senhas escritas e coladas no monitor, bem como o repasse de informações sigilosas em ambientes não seguros, como parada de ônibus, reuniões informais são situações muito comuns. Contar com a colaboração das pessoas é simplesmente fundamental para a empresa.Mas tudo deve ser auditado pelo CSO. Mas o ponto principal da preocupação com as pessoas é que os fraudadores irão em busca delas para perpetuar seus crimes.

Mas nem sempre as pessoas tem 100% de culpa, afinal, no mundo cibernético, tem muito lixo e armadilhas que foram projetadas justamente para enganar pessoas, ai fica muitas vezes difícil de controlar os processos que são confiáveis e não confiáveis, então cabe ao CSO orientar e auditar toda e qualquer mudança que possa possa colocar em risco os dados da corporação. Antivírus, anti-spywares, um bom proxy e um firewall são essenciais, mas nada melhor do que orientar e auxiliar os usuários no uso da tecnologia a favor da corporação..

Postado no vivaolinux - http://www.vivaolinux.com.br/artigos/impressora.php?codigo=8133
Recomendo a leitura do post:

- http://marcelokalib.blogspot.com/2008/04/procura-se-segurana-particular.html

Referências

Livros:

- PostgreSQL – Korry Douglas, Susan Douglas, SAMS, Capítulo 21
- PostgreSQL Developer's Handbook de Ewald Geschwinde, Hans-Jürgen Schönig , SAMS, Capítulo 6
- Boas fontes de informações: Capítulo 23 do livro PostgreSQL The Comprehensive Guide de Korry Douglas e Susan Douglas.

e Security and Access Restrictions no capítulo 6 do livro PostgreSQL Developer's Handbook de Ewald Geschwinde, Hans-Jürgen Schönig.

Riscos Envolvendo Informações
- Concentração das informações
- Permitir acesso indiscriminado
- Obscuridade
- Concentração de funções
- Falta de controle
- Retenção duradoura
- Relacionamento e Combinação de Informações
- Introdução de erros
- Lealdade
- Acesso não autorizado
- Perda da integridade

Principais Fatores de Segurança da Informação de Clare Less, Telecommucations, fev. 1989

Infra-estrutura

Separação de ambientes	Energia e ar-condicionado Radiação eletro-magnética	Proteção física

Recursos Técnicos - Integridade de dados - Confiabilidade - Integridade de programas - Gerenciam.de Recursos de PD	Segurança da Informação	Recursos Humanos: - Controle de acesso - Autorização de acesso - Identificação de usuários
	Manutenção - Proteção da privacidade dos dados - Salvanguardas legais - Organização	

Políticas de Segurança

Definir os Objetivos
Que deve constar?
- objetivos
- destino
- propriedade dos recursos
- responsabilidades
- requisitos de acesso
- responsabilização

- generalizações

Procedimentos
Softwares de segurança: firewals, anti-virus, antispy, etc.
Backups, mídias, local de armazenamento e acesso
Política de distribuição de e-mails
Logins e senha de usuários locais e de e-mails

Referência: Livro Segurança em Informática e de Informações, de Carso & Steffen