FACULDADES INTEGRADAS DE JACAREPAGUÁ

COORDENAÇÃO ACADÊMICA
CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"
EM ANÁLISE E GERÊNCIA DE SISTEMAS

Segurança de Dados

por

Patricia Vargas Rocha dos Santos Sá

Monografia apresentada em cumprimento às exigências para a obtenção do grau de Curso de Especialização em Análise e Gerência de Sistemas — Coordenação Acadêmica das Faculdades Integradas de Jacarepaguá — Pós-Graduação "Lato Sensu".

Rio de Janeiro
2001

AVALIAÇÃO DE MONOGRAFIA

Após o exame da Monografia da aluna Patricia Vargas Rocha dos Santos Sá atribuimos os seguintes graus:

Conteúdo: _____

Forma: _____

Avaliação Geral: _____

Média: _____

Rio de Janeiro, 18 de março de 2001.

Os Professores:

_____

Prof. Orientador da Monografia

_____

Prof. Coordenador

DEDICATÓRIA

Ao meu esposo Alessandro, em reconhecimento aos momentos roubados do nosso convívio, pela companhia nas noites em claro, pelo apoio e sacrifício feitos durante todo o curso.

AGRADECIMENTOS

Aos meus mestres durante o curso: Fabio Contarini Carneiro, Jaci Fernandeds, Claudio Passos, César Bezerra, Marcelo Paiva, Polyana Paiva, Ronaldo Goldschmidt, Vera Lúcia, Sergio Pacheco e André Luiz Varella Neves; ao coordenador Paulo Márcio e a secretária do curso Ana Paula.

SUMÁRIO

INTRODUÇÃO

Uma rede de computadores é formada por um conjunto deles, conectados uns aos outros, com capacidade de trocar informações e compartilhar recursos entre si.

Com a chegada das redes, vieram as preocupações com a segurança das informações que estariam disponíveis na rede; para solucionar este problema, começou-se a discutir segurança com diversos enfoques: segurança de dados/informações, de banco de dados, de sistema operacionais, na *internet*, quem nos ameaça e como ameaça.

Por fim, hoje no mundo cibernético temos as mesmas preocupações que temos no mundo real: Nosso carro será roubado no próximo cruzamento? Será que o *site* da empresa onde trabalhamos foi invadido?

É este ambiente de insegurança que estaremos analisando e procurando métodos de prevenção e defesa.

CAPÍTULO I - SEGURANÇA DE DADOS

1. Definição de Dado

O dado é o elemento básico do conhecimento. É através do processamento de um ou vários dados que obtemos a informação, principal orientadora no processo de decisão.

2. Definição de Informação

Num mundo tão competitivo como o mundo dos negócios, as informações devem ser tratadas pelas empresas como um dos seus maiores bens. As informações auxiliam na tomada de decisões que podem influir para o sucesso ou fracasso em algum negócio. Por isso, é importante que as empresas tenham um sistema de informações capaz de: fornecer dados consistentes que ajudem a fazer a previsão de situações e a planejar como lidar com elas.

3. Segurança de Dados

A fim de produzir uma informação consistente e correta, utilizamos os Sistemas Gerenciadores de Banco de Dados (SGBD's). Eles tem como função principal, coordenar e garantir o processamento dos dados iniciais, preservando com isso, a segurança e a integridade deles.

Para garantir a segurança e a integridade desses dados, algumas providências devem ser tomadas nos seguintes níveis:

3.1. Nível Físico

Falhas nos equipamentos de armazenamento, transmissão e processamento dos dados.

3.2. Nível Humano

Definição de níveis de acesso para cada usuário ou grupo de usuários.

4. Restrições ao acesso aos dados

Para maior integridade dos dados, deve-se prever o treinamento daqueles que utilizam os dados, permitindo a criação de rotinas para melhor administração dos mesmos.

Tendo em vista os fatores anteriores, podemos definir algumas rotinas para a administração dos dados, que irão produzir informações corretas e íntegras. A cada acesso a uma chave de dados, devemos seguir os seguintes passos:

- *Identificação de usuário:* o usuário tem em seu poder um nome de acesso (ou *login*) e uma senha; isso determina que ele tenha acesso a uma parte dos dados num todo.
- *Validação do usuário:* tendo seu *login* e sua senha validados, o usuário é transportado à sua área de acesso, onde ele tem seus dados disponibilizados com total controle.
- *Concessão de privilégios:* a concessão de privilégios visa, principalmente, a segurança dos dados, e é de competência do Administrador de Banco de Dados (DBA); mas não é somente o DBA que pode conceder esses privilégios; ele pode indicar um outro usuário para conceder privilégios acrescentando, no caso da Linguagem SQL (*Structured Query Language* – Linguagem de Consulta Estruturada, padrão em todos os SGBD's consultados e outros), o parâmetro *WITH ADMIN OPTION*, no comando de concessão de privilégios, isto é, uma política de administração de dados centralizada. Qualquer outro privilégio que venha a ser dado a outro usuário, tem que ser de conhecimento do DBA, pois é ele que, a princípio, concede tais privilégios e, quando há uma revogação dos mesmos, ele deve ser informado para que não provoque uma perda de privilégios injusta a usuários de nível inferior.

Temos também uma política descentralizada, onde somente os criadores dos objetos têm o poder de conceder privilégios de acesso a esses objetos.

Na figura abaixo, temos um exemplo simples onde o DBA concede privilégios a três usuários (Usuário 1, Usuário 2, Usuário 3), que por sua vez, podem também conceder

os mesmos privilégios dados a eles pelo DBA para outros usuários (Usuário 4, Usuário 5). Mas, para isso, diversos cuidados devem ser tomados, porque, no exemplo abaixo, o Usuário 1 concede privilégios ao Usuário 4 e ao Usuário 5, enquanto o Usuário 2, concede ao Usuário 5; portanto, se o DBA remover os privilégios do Usuário 1, os privilégios do Usuário 4 e Usuário 5 serão automaticamente revogados, mas, como o Usuário 2 também concede privilégios ao Usuário 5, este continuaria com seus privilégios.

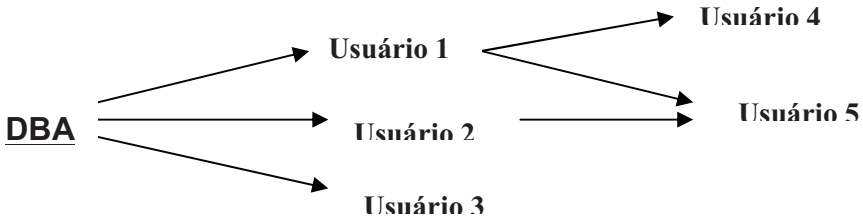


Figura 1

Ao adotarmos a concessão de privilégios, não estaremos garantindo requisitos suficientes para a segurança dos dados, sendo necessário adotar outros métodos para sua melhor segurança e confiabilidade. A criptografia, é uma das técnicas adotadas, para manter os dados ocultos, e possibilitar o sigilo das informações. Adiante, falaremos mais detalhadamente sobre criptografia.

- *Arquivos de Log:* o sistema deverá prever que a cada *login,* o usuário tenha seu nome, hora de acesso e, dependendo do sistema, o que ele realiza com os dados registrados em o que chamamos de *arquivos de log*. Em caso de má utilização de algum recurso do sistema, o encarregado de segurança, pode verificar quais foram os últimos acessos aos dados e, daí, obter os principais indícios de violação dos critérios de segurança dos dados.

CAPÍTULO II - SEGURANÇA EM BANCOS DE DADOS

A segurança das informações, como um todo, depende do esquema de segurança do banco de dados onde as mesmas estão armazenadas. Quando ela é quebrada, seja acidental ou propositadamente, os resultados são altamente prejudiciais; por isso, a segurança dos banco de dados é uma questão muito importante quando se desenvolve um projeto.

A base da segurança dos dados visa a proteger a integridade dos mesmos, ou seja, garantir que eles só sejam alterados ou excluídos por pessoas autorizadas a efetuar tais operações (usuário fonte). Todavia a segurança e a integridade dos dados não depende só das autorizações dadas a essas pessoas, mas sim, da maneira como se controla o acesso dessas pessoas, uma vez que elas podem, perfeitamente, contrabandear os dados que elas controlam. Podemos citar, como exemplo, a espionagem industrial.

O primeiro passo para a implementação da segurança no banco de dados, requer a garantia de uma política de privacidade e segurança, isto é, a definição do ambiente computacional que irá armazenar os dados (*hardware* e *software*), bem como do controle físico, humano e procedimental. Esta política vai definir o que deve ser feito e não como fazê-lo.

Em seguida, devemos mostrar os mecanismos que serão utilizados para cumprir as funções pretendidas pela política de segurança de dados.

O último passo a ser implementado é a garantia de que os mecanismos adotados cumpram, com um alto grau de confiabilidade, a política de segurança. Quanto mais alto for essa garantia, mais difícil será de quebrar a política de segurança.

Dentro de uma política de segurança de um banco de dados, devemos levar em consideração três principais objetivos:

- *Segredo*: prevenir o acesso às informações por usuários não autorizados, como por exemplo, em um sistema de folha de pagamento, onde um empregado inferior não deve ter acesso aos salários de seus superiores.
- *Integridade*: evitar modificações não autorizadas das informações, como por exemplo, nesse mesmo sistema de folha de pagamento, um funcionário alterar seu salário sem ser autorizado para isso.
- *Disponibilidade*: prevenir que algo empeça os acessos à informação, como por exemplo: nesse mesmo sistema de folha de pagamento, os cheques de pagamento devem ser impressos e entregues no prazo estipulado.

1. Tipos de Bancos de Dados:

1.1. Sistemas Centralizados:

Todos os dados ficam disponíveis em uma única unidade, e todos os serviços são executados diretamente na mesma. Facilita bastante a segurança, uma vez que os dados são armazenados em um só local.

1.2. Sistemas Descentralizados:

O banco de dados é dividido em partes, geralmente por setores ou áreas funcionais, tornando os dados mais facilmente disponíveis aos principais usuários. Apesar de não ser exatamente um banco centralizado, a segurança dos dados é feita basicamente como no modelo centralizado, uma vez que os dados, mesmo não estando armazenados em um só lugar, cada área funcional, é "centralizada" em um só local – o que da facilidade de controle nos acessos de cada área.

Os sistemas que utilizam bancos de dados tem sido feitos, tradicionalmente, de maneira centralizada. Dessa forma, o banco é armazenado em um único computador, onde são executados todos os programas que têm acesso ao banco.

Neste tipo de sistema, existe grande facilidade no controle de segurança e integridade dos dados.

Apesar de toda a vantagem em se poder manter os dados mais seguros, a centralização dos dados não atinge o principal objetivo que é a facilidade no acesso, ou seja, tornar o dado mais facilmente disponível à todos os usuários.

1.3. SGBD Distribuído

Um tipo de banco de dados que vem tomando destaque dentro do mercado empresarial, pois sua gerência, quando bem implantada, garante um bom cuidado com os dados, é o banco de dados Distribuído,

Um sistema de gerência de banco de dados distribuído é aquele no qual os dados podem ser armazenados em vários pontos da rede, sem que com isso ocorra divergência de informações.

A vantagem em se ter um SGBD distribuído é a facilidade de definir aplicações, com o partilhamento de recursos, *softwares* e informações, já que o sistema gerencia essas informações que se encontram dispersas, mantendo assim o controle de seus dados e aumentando a confiabilidade através da replicação das partes de maior importância do banco em mais de 1 ponto da rede.

Podemos também ser mais eficientes através de um critério de particionamento e replicação, no qual os dados mais utilizados fiquem mais próximos do local onde serão utilizados.

O SGBD distribuído terá que definir meios e critérios de autorização para acesso aos seus dados, garantindo com isso, também, a segurança dos seus dados.

Dentre as principais funções de um SGBD distribuído, temos algumas que tratam também da segurança dos dados. Dentre elas podemos citar, o controle de concorrência que tem como objetivo a garantia de que toda execução simultânea de um grupo de

transações, seja executada como se fosse a única no sistema. Em outras palavras, as transações não devem sofrer interferências que levem a anomalias de sincronização, como a perda de consistência do banco, e acesso à dados inconsistentes.

O controle de concorrência visa a garantir uma coisa muito simples: a individualidade das transações de um sistema, isto é, uma transação deve ser executada como se fosse a única do sistema. Uma transação só é inicializada após a anterior ser completamente processada.

Existem três técnicas de controle de concorrência:

- *Técnica de bloqueio:* bloqueia um dado pela transação, antes dele ser lido ou modificado. Essa técnica cria um *Deadlock* (bloqueio mútuo) que em ambientes distribuídos é difícil de ser resolvido.
- *Técnica de pré-ordenação:* é estabelecida uma prioridade de execução de transações, executando-as serialmente como se fossem escolhidas.
- *Técnicas Mixtas:* tentam combinar as vantagens das técnicas de bloqueio e pré-ordenação.
- *Técnica do Controle de Integridade:* nesta, o controle de integridade é implementado tanto como parte dos SGBD's globais, como dos SGBD's locais. Porém, as funções relacionadas às transações e consistências do banco são funções do SGBD global.

As falhas que podem ocorrer são divididas em dois tipos (*hardware* e *software*), ou seja, no processador local e nos periféricos que armazenam o banco e falhas na rede de comunicação de dados.

- *Técnica de Controle de Acesso ao Banco:* tem como objetivo a implementação de mecanismos que garantam a segurança dos dados armazenados, deixando que os mesmos sejam manipulados somente por usuários autorizados.

Esse controle de acesso restringe que um grupo de usuários tenha acesso a somente determinadas partes do banco de dados; assim sendo, esse usuário terá acesso ao banco através de sua visão.

O sistema deve oferecer também um mecanismo de autorização de privilégios, de forma que, quando o usuário entrar no sistema, ele seja identificado, e o sistema verificará se o usuário possui os privilégios necessários à execução do acesso.

1.3.1. Controles para Acesso aos Dados

Devemos levar em conta que controlar o acesso de usuários a um banco de dados, é assegurar que eles somente poderão realizar determinadas operações dentro de uma base de dados, se estiverem autorizados a fazê-las. Esses controles são baseados no fundamento de que um usuário tenha sido previamente identificado e autorizado a realizar operações com esses dados.

As linguagens SQL possuem os comandos *GRANT* e *REVOKE* que tratam da concessão de acesso aos dados. O primeiro fornece a um usuário os privilégios, enquanto o segundo, retira os privilégios (todos ou apenas alguns).

Alguns princípios de controle de acesso nos permitem realizar um controle mais consciente.

O controle discriminatório consiste em dar a diferentes usuários, diferentes tipos de acesso a diferentes objetos e dados, utilizando para isso comandos SQL. Atualmente, o padrão SQL permite que você conceda quatro tipos diferentes de privilégios que podem ser também combinados, para permitir um acesso totalmente diferente a cada tipo de objeto dentro de um banco de dados, são eles:

- *Insert (inserir):* permite a inserção de novos dados
- *Delete (apagar):* permite a remoção de novos dados
- *Read / Select (ler):* permite a leitura dos dados

- *Update (alterar):* permite a modificação dos dados

Outro aspecto importante no controle de acessos, baseia-se no conteúdo dos dados, isto é, mesmo que o usuário tente fazer algo que não é correto, mais que ele tenha permissão para isso, ele pode esbarrar em certos limites, chamados de visões.

Por exemplo: No sistema de folha de pagamento anteriormente citado, um usuário que tente alterar seu salário para R$ 30.000,00 pode esbarrar em uma visão que determine que o máximo a ser alterado naquela tabela, por aquele usuário, com aquelas permissões, é de R$ 15.000,00.

Outro método de controle importante é o "Acesso Mandatório Bel-LaPadula", onde cada objeto do banco de dados recebe um nível de classificação, que pode ser ultra-secreto, super-secreto, secreto, confidencial e público; e cada usuário recebe uma classificação em um nível de acesso igual a um dos níveis de classificação dos objetos.

Outro meio de segurança muito importante, quando se fala em banco de dados, trata-se de misturar ou codificar os dados para que, quando forem armazenados ou transmitidos por um meio de comunicação, não torne o banco vulnerável a acessos indevidos, não passando de bits inteligíveis. Esse processo chamado de criptografia é muito importante para a segurança dos banco de dados, uma vez que estes são armazenados por um longo período, em meios de fácil acesso.

1.4. Visão Atual de Segurança nos SGBBANCO DE DADOS Atuais

Dentre os SGBD's pesquisados, todos permitem uma linguagem em comum chamada SQL (Structured Query Language – Linguagem de Consulta Estruturada). Constatamos que, para cada SGBD, há uma funcionalidade diferente no que diz respeito à segurança, em seu aplicativo de manipulação.

Tomaremos como exemplo, para análise, os seguintes SGBD's:

- *Microsoft SQL Server 7.0* – Query Analyser
- *Oracle* – SQL Plus
- *IBM DB2* – Centro de Comando

Cada um desses Gerenciadores de Banco de Dados possuem suas ferramentas próprias e específicas para manipulação de dados; entretanto, alguns utilizam sistemas diferentes quanto à segurança de dados.

1.4.1. Segurança no MS SQL Server 7.0

O manual de segurança do *MS SQL server 7.0*, descreve que a segurança deste SGDB é baseada no modelo de segurança do *Windows NT*, dessa maneira, vamos comentar um pouco da segurança do *Windows* no decorrer deste texto.

O SQL 7.0 possui dois modos para garantir a segurança no acesso ao servidor, que são: *Windows NT Authentication Mode* (mode de autenticação do *Windows NT*) e *Mixed Mode* (modo misturado).

Trataremos agora, separadamente, estes modos de segurança:

1.4.1.1. Windows NT Authentication Mode

Neste modelo de segurança, os administradores criam usuários e grupos de usuários no diretório de usuários do *Windows NT*, e dão a esses usuários e grupos, permissões de acesso ao SQL 7.0.

Quando o modelo de autenticação do *Windows NT* é utilizado, o DBA permite que os usuários tenham acesso ao comutador que está executando o *SQL Server*, garantindo a eles o direito de se *logar* no *MS SQL Server 7.0*. Os acessos são autenticados através dos identificadores de segurança do *Windows NT* (SIDs). Assim, quando esses identificadores são utilizados, o DBA pode garantir o acesso ao SQL diretamente para usuários e grupos

de usuários no *Windows NT*, sem a necessidade da criação de contas de acesso para os mesmos no *SQL 7.0*.

A concessão de acesso aos usuários deverá ser feita da seguinte maneira:

1.4.1.2. Windows NT

No *Windows NT*, os administradores devem criar contas de acesso para cada usuário, concedendo permissão de acesso ao *SQL Server* à cada um deles. Para os que já possuem conta, basta conceder a permissão.

Após a criação das contas, podem ser criados grupos globais, onde os usuários serão agrupados de acordo com suas necessidades de acesso ao SQL. Nesse caso, no computador em que o SQL está sendo executado, devem ser criados grupos locais de acordo com as necessidades de acesso que devem ser concedidas ao *SQL 7.0*. Depois, os grupos globais devem ser inseridos nos respectivos grupos locais na máquina onde o SQL está sendo executado. O objetivo é que todos os usuários, com os mesmos requisitos de segurança, sejam agrupados para que o administrador possa garantir-lhes acesso. Porém, garantir o acesso ao SQL através de grupos, não impede que os usuários sejam identificados separadamente, uma vez que as ações de cada um são armazenadas em um arquivo de *log*.

1.4.1.3. MS SQL 7.0

No *SQL 7.0*, devem ser concedidas, aos grupos locais criados no *Windows NT*, permissões de acesso ao SQL. A permissão de acesso pode ser concedida a cada usuário separadamente, mas esse procedimento não é fácil para se administrar, quando se tem grande quantidade de usuários.

1.4.1.4. Mixed Mode

Nesse modelo, os usuários também podem ser autenticados diretamente através do *Windows NT*, da mesma maneira que era feito através do *Windows Authentication Mode*.

No entanto, os usuários deverão fornecer ao SQL um *username* e uma senha, que serão comparados com os armazenados em suas tabelas de sistema. Este tipo de conexão é chamado de *non-trusted conection* (conexão não confiável).

Esse sistema de conexão não confiável, só é recomendado quando o *SQL 7.0* está instalado sobre o *Windows 95/98*.

Para garantir o acesso ao SQL através de conexões não confiáveis, devem ser criadas contas para cada usuário diretamente no *SQL 7.0*.

1.4.2. Segurança no ORACLE

A segurança dos dados no *Oracle* possui aspectos muitos avançados, pois controlam como um banco de dados é usado e acessado, prevenindo assim o acesso a um banco de dados e seus objetos por usuários que não tem autorização; além de controlar o uso do espaço e dos recursos disponíveis, fazendo também auditoria das ações dos usuários.

Há duas c*ate*gorias de segurança no *Oracle*:

- *Segurança do Sistema:* aquela em que os mecanismos de segurança controlam os acessos ao banco de dados a nível de sistema, ou seja, controlam a validação do nome e a senha do usuário, os espaços disponíveis em disco para a criação e controle de objetos, o limite dos recursos, a auditoria dos mesmos e as operações que o usuário pode executar.
- *Segurança dos Dados:* aquela em que os mecanismos de segurança controlam os acessos do banco de dados a nível de objetos, ou seja, criar privilégios e restrições aos acessos às informações. Isto é feito concedendo um privilégio apropriado a cada usuário para um determinado objeto

Operacionalmente a confidencialidade no SGBD *Oracle* está baseado nos seguintes parâmetros:

1.4.2.1. Autenticação e identificação do usuário

Antes da conexão com o banco de dados, o *Oracle* faz a validação do usuário através de sua identificação (*login* e senha).

1.4.2.2. Controle de Acesso Discriminatório

Faz a restrição dos usuários permitindo a realização de determinadas operações e de acessar determinados objetos no banco de dados através de privilégios.

1.4.2.3. Controle de Acesso Mandatório

Faz a restrição de acesso dos usuários através da classificação dos objetos. O sistema rotula e armazena os objetos a fim de atribuir classificações. O usuário só pode acessar o objeto cuja informação não seja confidencial no seu nível.

1.4.2.4. Auditoria

É a gravação das operações executadas no banco de dados e os respectivos usuários que as executam, com o objetivo de gerar um "arquivo de auditoria" que pode ser analisado a qualquer hora para detectar ameaças de segurança e descobrir possíveis causadores de danos aos dados. O *Oracle 7* fornece opções de auditoria por usuário, por operação no banco de dados, por objeto acessado e por privilégio de sisterma.

1.4.2.5. Encriptação no B*banco de dados*

Cada banco de dados no *Oracle* é armazenado de uma forma codificada que só pode ser decifrada com o *software* específico e a chave de decodificação correta.

1.4.3. Segurança no IBM DB2

O banco de dados da IBM DB2 é um banco não muito conhecido nos ambientes universitários e em plataformas *Desktop* (para PC's domésticos), mas em grandes empresas ele é altamente conceituado, ainda mais nos micros AS400, também de fabricação da IBM.

O motivo da grande utilização dele nas grandes empresas (mais ainda perde grande terreno para a *Microsoft* com o *SQL Server* e para a *Oracle*) é o fato de que ele ainda é o mais barato dos três, e que ele é praticamente automático se for corretamente configurado, pois ele tem diversos assistentes para realizar trabalhos complexos que tomariam uma grande quantidade de tempo do DBA, fazendo com que ele se dedique quase que somente a supervisionar o banco de dados.

Uma de suas desvantagens é que se você precisa alterar um determinado valor de um dado, você utilizará o SQL, que passará a se tornar um exercício de paciência pois o centro de controle do DB2 (onde trabalhamos com a SQL) executa os comandos um à um, isto é, você digita uma linha e executa, fazendo esse procedimento até o final do seu comando.

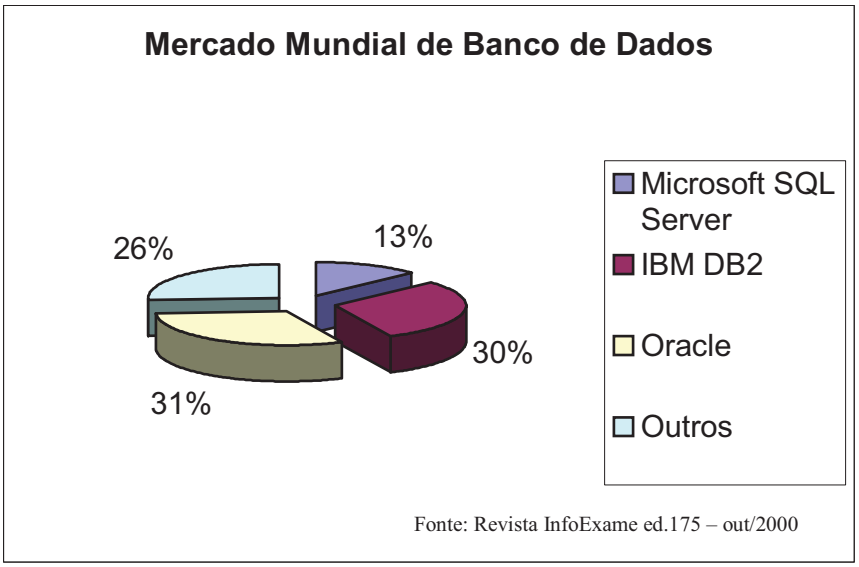
1.4.3.1. Segurança

Como em todos os bancos de dados anteriormente pesquisados, a segurança do DB2 se limita somente a processos de autenticação e autorização de usuários combinados a sistemas de segurança externos (os dos Sistemas Operacionais).

A autenticação é a ação que o usuário faz de fornecer um nome e uma senha, que após comparados com os armazenados no banco central do DB2 permitem o acesso ao usuário. Após isso ele passa a ser autenticado, isto é, todas as tabelas, e tipos de permissões que aquele usuário tem são concedidas para que ele de inicio ao seu trabalho.

Existem dois tipos de autorizações no DB2: os privilégios e os níveis de autorização. Um privilégio define uma permissão simples ao usuário, isto é, ele pode criar e acessar recursos do seu banco de dados. Os níveis de autorização entretanto dizem respeito a um controle de privilégios de grupo atribuindo a um usuário dentro de um grupo o poder para conceder privilégios.

Além desses princípios básicos de segurança, o DB2 também fornece meios para realizar encriptação de dados em transmissões e auditoria de acesso. Métodos simples como esses associados a métodos de segurança dos Sistemas Operacionais fazem do DB2 um SGBD seguro, desde que haja um bom treinamento em Administração do Banco.



Fonte: Revista InfoExame ed.175 – out/2000

CAPÍTULO III – SEGURANÇA EM SISTEMAS OPERACIONAIS

1. Introdução

Neste capítulo, iremos abordar os principais Sistemas Operacionais e seus aspectos voltados para segurança; os principais problemas que comprometem a segurança dos dados; como identificar, prevenir e solucioná-los.

Falaremos primeiramente das "brechas" nos Sistemas Operacionais; o que elas são; de onde vêm e o que você pode descobrir sobre elas; erros ou "*bugs*" que geram novas "brechas", e o que os principais fabricantes geram em matéria de correções.

Iremos abordar um esquema padrão numa Política de Segurança confiável, dentro de uma empresa, para depois aplicarmos esse esquema dentro de cada sistema operacional.

2. Brecha

A "brecha" nada mais é do que um "*bug*" em qualquer *hardware*, *software*, ou Diretiva de Segurança, que expõem as vulnerabilidades do seu Sistema Operacional, ou da sua rede, permitindo acesso não autorizado, comprometendo os sistemas e as ferramentas que compõem uma rede, dentre as quais podemos citar: Roteadores e os *Firewalls*.

Com o avanço da *Internet* no mundo, a divulgação de uma brecha, ocorre em questão de poucas horas, fazendo com que pessoas mal intencionadas, como os *Crackers* se aproveitem dessas Brechas para gerar danos aos sistemas, ou até mesmo uso em proveito pessoal.

Se você não quiser deixar sua rede totalmente exposta, fique ligado no mundo externo quanto as atualizações e às novas brechas que vão sendo descobertas a cada dia, para posterior prevenção.

2.1. Como surgem as Brechas

As “brechas” não aparecem sozinhas, elas são descobertas. Quem as descobre está incluído em um dos seguintes grupos: os c*rakers*, os *hackers* e as equipes de segurança dos fabricantes.

Dependendo de quem as descubra, essa informação pode ser distribuída ao público de diferentes maneiras:

- Caso a descoberta venha dos *crackers*, a primeira notícia que recebemos é sobre um bando de servidores invadidos em cima daquela brecha, que foi descoberta;
- Se forem os *hackers* quem as detectou, essa informação chegará através de recomendações em boletins de segurança, ou por meio de revistas e de jornais especializados, ou na própria *Internet*;
- No caso das equipes de segurança dos fabricantes, essa informação é sempre a última a chegar na mídia, pois já aparece acompanhada da solução.

3. Políticas de Segurança em Sistemas Operacionais

A implementação de uma política de segurança confiável, está relacionada a criação de usuários. Temos que ter em mente antes da criação desses usuários ou grupo de usuários, quais recursos da rede (arquivos e diretórios) eles terão acesso.

O administrador da rede deverá ter controle total sobre esses usuários e sobre os recursos que serão utilizados por eles.

Para definir as restrições e privilégios que serão aplicados aos usuários, o administrador da rede deve conhecer as funções e as necessidades de cada usuário no contexto geral da empresa.

Dentro da definição dos privilégios e das restrições, está o compartilhamento dos recursos de rede; por exemplo: em um sistema centralizado definimos quais pastas serão compartilhadas e quais usuários terão as devidas permissões de acesso a esses recursos.

Fica a critério do administrador de rede qual é a medida que ele irá adotar para a proteção dos arquivos mais importantes dentro de sua rede; ou ele vai validar o acesso do usuário, ou vai colocar senhas para acesso também a uma determinada pasta, com a validação inicial do usuário (*login*); ou dependendo da importância do arquivo final, ele pode acrescentar mais uma senha para acesso (acesso mandatório).

Além da colocação excessiva de senhas, o arquivo também pode ser criptografado, fazendo com que além da senha de acesso, haja uma chave de acesso que se encarrega de desencriptar o arquivo assim que ele chega no seu destino. Assim, se ele for interceptado no meio de uma transmissão, não passará de um monte de letras sem sentido para aquele que o interceptou.

Mas, o mais importante de tudo, independente dos níveis de proteção para um arquivo/conjunto de arquivos, é que seja administrado dentro da empresa, ou local onde esteja sendo implantado a política de segurança; todos devem ter em mente que a melhor medida de segurança possível é a velha e boa senha; ela deve ser bem escolhida e pode seguir umas pequenas regras de criação que aconselharemos mais adiante.

Outro fator a ser levado em consideração é o fato de que não importa a segurança que você tenha, você pode sofrer as conseqüências de uma invasão, e se isso acontecer o que deve ser feito?

Primeiramente, ver o que foi danificado ou perdido e restaurar, através das últimas cópias de segurança (*backup*) que você dispõe. Por isso, uma política de *backup* deve ser implementada entre os componentes de um CPD, respondendo perguntas simples, tais como as citadas abaixo, você pode criar boas rotinas de *backup* e ter seus dados sempre atualizados.

- De quanto em quanto tempo esse *backup* vai ser feito?
- Quais serão os arquivos/pastas a serem copiados?

- Como ele será feito (periodicidade)?
- Para onde ele será feito (meio físico)?

Através das respostas a essas simples perguntas, teremos uma boa maneira de recuperarmos-nos de ataques que danifiquem as informações da empresa.

Por mais que você (administrador de rede, banco de dados, CPD etc) fale sobre o perigo dos vírus, sempre vai existir aquela pessoa que pensará que isso nunca vai acontecer com ela, e trará para o local de trabalho, ou levará para casa aquele disquete de procedência duvidosa, ou abrirá aquele e-mail do amigo ("Ele é meu grande amigo, nunca me mandaria vírus"), e então era uma vez uma rede de computadores. Por isso, mantenha o antivírus de sua empresa sempre atualizado, verifique constantemente os boletins de segurança existentes na *Internet*, e leia as revistas especializadas no assunto, pois elas sempre trazem notícias sobre os novos vírus, seus eficientes meios de propagação e seu grande poder de destruição.

Resumindo, o principal fator de sucesso para a implementação de uma política de segurança eficiente, ainda é a conscientização de todos os setores da empresa de que segurança não é uma coisa barata e que requer um investimento significativo.

Geralmente, quando não ocorre situações danosas de perda e/ou violação dos dados, esse investimento parece que foi feito em vão; porém, quando não é feito o investimento necessário e ocorre o prejuízo por uma invasão, as perdas geralmente são incalculáveis. Por isso, a pessoa que é responsável pela informática dentro da empresa deve saber como mostrar a todos que a segurança da informação é uma coisa que afeta a todos, e todos têm que ter a mesma preocupação e responsabilidade.

Em tempo: Até aqui estamos falando sempre em nível de empresa, administrador de rede e etc, mas todos os conceitos e dicas descritos e os que vêm daqui pra frente,

deverão ser de extrema atenção, também pelos usuários "domésticos" (aqueles que só usam, ou só tem os PC's em casa), já que com o avanço e a chegada rápida da *Internet* às casas, existirão pessoas que terão um equipamento muito mais vulnerável em casa do que em qualquer empresa e, por isso, tem que tomar as medidas necessárias para ter um computador bom e seguro.

4. Atualizações

Uma maneira de manter o seu sistema operacional seguro é mantê-lo atualizado. Atualizações são pequenos arquivos (pequenos em relação ao tamanho total do sistema operacional) que contêm correções de *bugs* e aprimoramento de segurança e de sistema.

Para cada sistema operacional, você deve seguir uma caminho diferente para encontrá-lo, as atualizações do *Windows 98/Me* podem ser encontradas na página do *Windows Update* (windowsupdate.microsoft.com) ou em cd's de revistas especializadas e vêm com o nome de correções; já para o *Windows NT/2000*, podemos encontrar as atualizações na própria página da *Microsoft* (www.microsoft.com/windows/nt) com o nome de *Service Pack* (mais a frente veremos alguns detalhes); para o *Linux,* você vai encontrar as atualizações na página do distribuidor da sua versão do *Linux* ou nas próximas versões do cd.

Particularmente, a *Microsoft* tem uma estratégia de mercado muito interessante; ela anuncia fofocas sobre o seu novo sistema operacional, e quando a lança, vende tudo o que quer; mas aí, os *bugs* vão aparecendo, e se a quantidade é muita, ela lança uma segunda versão do Sistema Operacional os chamados "Segundas Edições"; por isso, se você usa um sistema operacional da *Microsoft*, espere pela segunda edição dele, se você quer se livrar de pequenos problemas.

4.1. Dicas para se criar uma senha segura

Por melhor que você conheça os dispositivos mais avançados de segurança existentes no mercado, nunca deveremos esquecer que uma senha bem elaborada resolve praticamente 90% dos problemas de qualquer pessoa/empresa. Abaixo, daremos algumas dicas do que fazer e o que não fazer em relação as senhas.

4.1.1. O que não fazer

- Colocar nomes pessoais ou de pessoas famosas;
- Colocar números ou letras repetidas; (ex.: 5555, kkkk, etc)
- Colocar números de documentos principais (RG, CPF...) ou datas comemorativas (aniversários, casamentos etc)
- Repetir o nome colocado como *login* ou coloca-lo de trás pra frente.

4.1.2. O que fazer

- Misturar letras e números, e quando o sistema operacional fizer diferença por letras maiúsculas e minúsculas (ex.: *Linux*), também as utilizar;
- Usar símbolos ou caracteres especiais (tabela ASCII), tais como, %,#,*,^,€, etc;
- Quando puder, utilizar de senhas grandes, pois quanto maior é a sua senha mais difícil de ser quebrada; mas cuidado, ela também pode ser mais difícil de ser lembrada.

Com essas pequenas dicas não garantimos que você vai ficar 100% seguro, mas irá evitar pelo menos 80% dos problemas referentes a invasões.

Abaixo, segue a notícia sobre o primeiro evento computacional envolvendo Kevin Mitnick, para quem não sabe Kevin é o mais famoso dos *crackers* conhecidos, ficou famoso quando em 1990 roubou mais de 20.000 números de Cartão de Crédito e os distribuiu pela *Internet* e sumiu sem deixar vestígios dando muito trabalho ao FBI que levou mais de 5 anos para encontrá-lo e prendê-lo. Ele foi o primeiro *cracker* a entrar na

lista dos 10 mais procurados do FBI, e depois de 4 anos e meio de prisão, atualmente se encontra em liberdade condicional e trabalha como consultor de uma revista de informática

"MITNICK DA PRIMEIRA PALESTRA DEPOIS DE LIBERTADO

Fonte: The Standart, 28/09/2000

Depois de quatro anos e meio de prisão e alguns meses de liberdade condicional, o famoso cracker Kevin Mitnick deu sua primeira palestra durante conferencia sobre e-Business promovida pelo Giga Research's Infrastructures. Mitnick defendeu que o treinamento de funcionários sobre boas praticas de segurança pode ser mais importante que qualquer tecnologia de ponta. "As pessoas são o elo mais fraco", disse. Ele citou como exemplo crackers que muitas vezes enganam alguém de uma empresa para obter senhas e dados confidenciais, prática conhecida como "engenharia social".

Preso em fevereiro de 1995, Mitnick esta impedido de falar sobre o seu processo judicial e de usar computadores até 2003, condições para se manter em liberdade condicional. O cracker já havia recebido algumas propostas de trabalho como escrever sobre segurança num site e comandar um programa de radio.

Leia algumas recomendações de Mitnick:

- *Confirmar a identidade antes de fornecer informações;*
- *Não escolher senhas obvias ou que formem palavras;*
- *Não escrever senhas em papeis ou em lugares de fácil acesso;*
- *Trocar de senha freqüentemente;*
- *Usar senhas diferentes para cada sistema;*

- *Usar triturador de papeis para destruir documentos;*
- *Destruir CDs e disquetes, já que dados apagados podem ser recuperados.*

Fonte: Newsletter da Módulo – www.modulo.com.br

5. Linux

Criado pelo universitário finlandês Linus Torvalds em 1991, o *Linux* é atualmente utilizado por grandes empresas (e até governos), principalmente em aplicações ligadas a *Internet*.

A segurança no *Linux*, assim como de qualquer outro sistema *Unix*, deve ser vista de um modo diferente de um sistema *Windows*. No *Linux*, um administrador deve preocupar-se em saber quais os problemas (*bugs*) existentes em toda a base de software instalada. Tais problemas podem facilitar o acesso de usuários maliciosos a todo o sistema.

Discutiremos alguns tópicos importantes relacionados a segurança deste moderno sistema operacional como:

5.1. Controle de acesso

O sistema de gerenciamento de arquivos do *Linux* permite restringir o acesso aos arquivos e diretórios, associando a eles um conjunto de permissões ou privilégios. Essas permissões determinam quais arquivos o usuário pode ler ou manipular. Cada usuário assume um ou mais papéis com relação ao arquivo:

- *Proprietário ou usuário:* o usuário é o dono do arquivo (geralmente o seu criador). O proprietário é quem define as permissões para o arquivo.
- *Grupo:* o usuário pertence a um grupo de usuários relacionado ao arquivo. Neste caso, o arquivo pode ser controlado por várias pessoas ao mesmo tempo.
- *Outros:* o usuário não é o dono do arquivo e nem pertence a um grupo relacionado a ele.

Para cada um desses papéis são definidas as permissões de acesso:

- *Leitura:* permite que o usuário leia o conteúdo de um arquivo;
- *Escrita:* permite que o usuário modifique o conteúdo de um arquivo;
- *Execução:* permite que o usuário execute um programa ou realize buscas dentro um diretório.

Exemplo: Vamos agora a um exemplo que demonstre como são representadas as permissões sobre um arquivo:

-rw-r--r-- 1 root root 743 Jul 31 1994 texto.txt

Acima podemos ver os atributos dos arquivos e diretórios (tamanho, data e hora da última modificação), seu proprietário, a que grupo está relacionado e as permissões. As permissões de leitura, escrita e execução são representadas respectivamente pelas letras ‘r’, ’w’ e ‘x’. E quando uma permissão é negada isto é representado por um ‘-‘. Veja as permissões sobre o arquivo texto.txt na tabela abaixo:

Tipo de arquivo	Proprietário			Grupo			Outros		
-	r	w	-	r	-	-	r	-	-

A primeira coluna da tabela informa o tipo de arquivo: ‘d’ para diretório, ‘l’ para link e ‘-’ para outros arquivos.

A segunda coluna corresponde aos privilégios do proprietário do arquivo e neste caso, ele tem permissões de leitura e gravação sobre o arquivo texto.txt.

A terceira e a quarta coluna correspondem, respectivamente, aos privilégios do grupo o qual este arquivo está relacionado, e os outros usuários do sistema. Eles possuem apenas permissão de leitura sobre o arquivo texto.txt.

5.2. Segurança de senha

A segurança de senha do *Linux* é confiável quando ela é implementada corretamente. Além de educar seus usuários a criar senhas difíceis de serem adivinhadas, o administrador deve também utilizar utilitários preventivos de senha, sombreamento de senha e empregar a criptografia onde for possível.

O objetivo de um programa de verificação de senhas preventivas é impedir que o usuário crie senhas fracas, isto é, senhas que podem ser facilmente adivinhadas ou "craqueadas". Quando o usuário insere uma senha, o programa a compara com uma lista de palavras e um conjunto de regras. Se a senha digitada não atender aos requisitos do programa, o usuário terá que escolher uma outra.

No sistema *Linux*, as informações do usuário são guardadas no arquivo *password*, localizado no diretório /etc. Esse arquivo contém nomes de *login*s, nomes de usuários e as suas senhas (na forma criptografada).

Embora a senha esteja criptografada, nada impede que alguém tente quebrá-la. Com o sombreamento de senhas, a senha criptografada é escondida em outra parte da unidade; e no arquivo *password*, no lugar da senha criptografada, será encontrado um caractere que será uma representação abstrata desta senha.

5.3. Segurança da conta Root

O *root* (raiz) é uma conta administrativa especial que concede acesso irrestrito a todo o sistema. O *root* corresponde à conta administrador no NT e de supervisor no *Novell*.

Essa conta pode executar operações irreversíveis ao sistema, por isso é aconselhável utilizá-la somente quando for absolutamente necessária como por exemplo: configurar algum dispositivo ou instalar algum programa.

A existência de uma conta privilegiada pode ser considerada uma ameaça à segurança. Por possuir controle total do sistema, o *root* é o principal alvo de crackers; se o *root* for comprometido, sua rede também será.

A segurança do sistema inicia-se no momento da instalação do Linux, quando é solicitada a configuração de senha de raiz. É verdade que distribuições, como o *Red Hat Linux*, forçam a atribuição de uma senha antes da primeira inicialização. Porém o *Linux Slackware* permite que se efetue *login* de *root* sem uma senha quando a instalação está completa. Então se torna obrigação sua configurar esta senha.

No entanto, um *cracker* nem precisa efetuar *login* de *root*, apenas adquirir privilégios dele. Para isso o *cracker* se aproveita de *bugs* de programas que precisam ser executados como *root*. Quando o programa é atacado, concede ao seu atacante os privilégios de *root*.

Por isso é importante manter-se atualizado sobre o surgimento de novas falhas e as suas correções.

Serviços

O Linux possui alguns serviços que podem deixar o seu sistema vulnerável a ataques, ainda mais se estes programas estiverem com versões desatualizadas.

Quando o seu computador é ligado estes serviços podem ser inicializados pelo programa *inetd* ou pelos arquivos dentro do diretório de inicialização do Linux, chamado *rc.d*.

Cabe ao administrador do sistema verificar se estes serviços são realmente necessários a sua rede e, se não, desabilitar estes serviços. Caso haja necessidade de algum destes serviços, que ele utilize sempre a versão mais atualizada deste software. Veja agora algum destes serviços:

- *Telnet*: É um serviço que, não apenas permite ao usuário efetuar *login* em um *host* remoto, como também execute comandos nesse *host*. Exemplo: uma pessoa na cidade A pode acessar uma máquina na cidade B e executar programas na máquina da cidade B como se ele estivesse nessa cidade.

O Telnet pode ser usado de inúmeras maneiras para atacar ou colher informações importantes de um *host* remoto. Contudo se o administrador pretende fornecer a seus usuários acessos de Telnet, ele deve estar *até*nto aos *bugs* de seus servidores de Telnet.

Um exemplo de Telnet vulnerável vem do *Red Hat Linux 4.0*. O pacote de Telnet em distribuições *Red Hat Linux 4.0* irá cortar a conexão se o nome de um usuário dado for inválido. Contudo, se o nome do usuário for válido, mas a senha estiver errada, o servidor emitirá novamente um *prompt* de *login*, podendo assim dar a um *cracker* mais uma chance de se conectar.

- *Finger:* É um serviço comum para os sistemas UNIX. Ele fornece informações importantes sobre usuário (*login*, nome do usuário, diretórios etc) para *hosts* remotos e, como todo servidor TCP/IP, o Finger tem por base o modelo cliente-servidor.

O servidor de Finger, chamado Fingerd, quando recebe uma solicitação de algum usuário (seja ela local ou remota) encaminha qualquer que sejam as informações do usuário alvo que estão atualmente disponíveis.

Por isso muitos administradores não oferecem este serviço.

Existem outros serviços inseguros, como o *lpd, apm, dhcpd, nfs* e *smb*, que se não estiverem sendo utilizados nas suas versões mais atuais, podem servir como uma brecha para que qualquer invasor.

Open BSD

"Seguro até na instalação padrão". É isto o que promete o Open BSD, que ao contrário de outros sistemas não precisa de configurações complicadas para se obter o mínimo de segurança.

O Open BSD é um sistema gratuito, multiplataforma e multiusuário. Seu código-fonte é extensivamente auditado por profissionais de segurança e sua criptografia implementada no próprio SO.

Está disponível no sistema o IPSEC, protocolo utilizado para estabelecer VPN (*Virtual Privaté Network*) e protocolos como o *Openssh*, para realizar conexões criptografadas entre as máquinas da mesma rede.

Windows NT 4.0

O Windows NT é o Sistema Operacional – SO de redes mais utilizado no mercado corporativo devido à tendência de Centralização de dados, que por sua vez, está crescendo muito, principalmente no mercado Nacional.

Devido ao fato do Windows NT ser um SO muito utilizado, ele atrai a *até*nção tanto de especialistas em Segurança, como dos *Hackers*. Com isso surge diversas brechas de segurança.

Contudo, se o sistema for adequadamente configurado, ele se mostra um sistema altamente seguro.

Corrigindo as falhas

Para uma segurança confiável, é essencial que as máquinas estejam utilizando versões mais atuais do SO. Por isso, é que a maioria dos fabricantes disponibilizam dessas atualizações gratuitas, via *Internet*.

Service Pack

No Windows NT, as atualizações são conhecidas como *Service Packs* (SP) e contém correções de erros, melhoramentos e novas características do sistema. Os SP são acumulativos, por exemplo, o SP 3 incorpora todas as alterações dos SP 1 e 2. A instalação do SP mais recente é um sistema de segurança obrigatório para uma boa política de segurança em redes. O último SP é o de número 6.

A microsoft lançou em 1985, o seu primeiro software de rede, chamado PC-LAN, permitindo a usuários do MS-DOS compartilhamento de diretórios e impressoras através de uma rede local. A segurança era precária, pois contava somente por uma senha única em que podia ser colocada em cada compartilhamento. Era mais adequado para micros como na época eram chamados, mais ainda distante do que era oferecido por SO mais avançados como o VMS e o UNIX.

Com o seu razoável funcionamento e oferecimento de recursos pouco fornecido, foi o que motivou mais investimentos da Microsoft na área. A cada novo produto lançado no mercado, foram adicionados mais recursos, tornando o que era um protocolo simples, em um conjunto de rotinas bastante complexos. Ao conjunto de compartilhamento de recursos, autenticação de usuários, *browsing* e resolução de nomes, chamamos de "Rede Microsoft".

Autenticação no Windows NT

No ambiente NT, quando o usuário se "loga", significa que ele foi identificado pelo Windows NT, sendo assim ele pode ter acesso aos recursos da máquina.

Por "*login*" entendemos, o fornecimento de um nome de usuário e uma senha específicos da pessoa que estava utilizando a máquina. Após isso, essa informação é checada no registro de usuários local e se correta, o usuário é autenticado ou "logado".

Tipos de "*login*", são três:

- *Login Local:* quando o usuário está utilizando a máquina que contém o Windows NT, fazendo *login* direto (teclando CTRL + ALT + DEL e informando conta e senha).
- *Login pela Rede:* quando o usuário informa seus dados por uma estação de trabalho e é autenticado pelo servidor de rede.
- *Login como Serviço:* quando um serviço se identifica para executar com as permissões de um determinado usuário.

Após o "*login*", os usuários são associados a uma série de privilégios determinando a utilização ou não de diversos serviços do sistema, esses privilégios estão contidos em um "token" (bastão) que o usuário recebe assim que se "loga", você pode ver estes privilégios e quem os possui, através da ferramenta "Gerenciadores de Usuários" (User Manager).

Uma boa medida de segurança é você, atribuir o *login* local apenas aos usuários que vão se utilizar mais do console da rede, por exemplo: aos administradores, operadores de backup, DBA's e etc. Negando o acesso aos demais usuários considerados "simples", que irão se utilizar apenas das máquinas clientes.

Implementando uma política de Senha

Para implementação de uma boa política de Senha, primeiramente devem ser seguidas as dicas anteriormente ditas no inicio do capítulo.

Através da ferramenta "Gerenciamento de Usuários", você pode definir uma política de senhas a ser utilizadas pelo NT, como por exemplo:

- Fornecer um período de velocidade de senhas para que o usuário a troque obrigatoriamente e periodicamente.
- Permitir que o usuário não se utilize de senhas anteriores (o sistema guarda todas as últimas 10 senhas utilizadas pelo usuário.
- Bloquear a conta do usuário após um determinado número de senhas incorretas (sendo desbloqueada somente pelo administrador ou por um determinado período de tempo).

Essa opção é altamente importante devido a uma grande falha na auditoria do NT, no caso de um "*login*" incorreto ele não registra o endereço de onde foi feita a tentativa.

A partir do Service Pack 2 do NT 4.0, pode forçar os usuários a se utilizarem de "senhas fortes", isto é, difíceis de serem adivinhadas. Este SP vem com um arquivo que obriga as senhas a terem pelo menos um caracter de no mínimo três das quatro c*até*gorias abaixo:

- Letras maiúsculas e minúsculas
- Números e Caracteres Especiais
- Pontuação.

Para habilitar este arquivo, edite o registro utilizando o REGEDIT ou REGEDT32 e edite a chave HKEY_LOCAL_MACHINES\SYSTEM\ CurrentControlSet\System\CurrentControlSet\Control\LSA. Crie o valor *Notification Packages*, do tipo REG_MULTI_SZ, caso ele ainda não exista, e adicione ao seu conteúdo a string "PASSFILT".

Auditoria

Por exigência de Órgãos Internacionais de Segurança, todas as ações do sistema no Windows NT, podem ser registradas e auditadas. Ações como acesso a arquivos, "*login*" de usuários, execução de programas e impressão de arquivos. Sendo de fundamental importância, para a verificação de problemas e defeitos, bem como também coordenar a integridade e a segurança do sistema.

Os registros gerados pela auditoria são acessados pelo "Visualizador de Eventos" e são divididos em três tipos diferentes: Sistema, Segurança e Aplicativo.

Após a instalação o Windows NT, devemos habilitar a opção de auditoria por segurança, que vem por padrão, desligados.

Na janela de configuração de Política de Auditoria podemos registrar as seguintes ações, tanto no sucesso (o usuário estava autorizado a faze-la) como em caso de falha:

- *Logon e Logoff:* Registra o sucesso ou falha na autenticação de um usuário durante o *login*, e também a sua saída do sistema, após ativada, está opção permite saber quais usuários estavam usando o sistema em um determinado período de tempo, e se alguém está tentando usar indevidamente a senha de outro usuário.
- *Acesso a Objetos e Arquivos:* Registra o acesso (ou tentativas de acesso) aos arquivos e outros objetos do sistema, como compartilhamentos, *pipes* e a *registry*.
- *Uso dos direitos do Usuário:* Ao ser acionado será registrado o uso de privilégios do sistema por parte dos usuários, como mudar a hora do sistema, acrescentar uma máquina no domínio ou tomar posse de arquivos.
- *Administração de usuários e grupo:* Se refere a qualquer alteração na base de usuários do sistema, como inclusão e deleção de usuários, ou alteração de senhas.
- *Troca de Políticas de Segurança:* Alterações nos privilégios dos usuários ou na política de auditoria do sistema.
- *Reiniciar ou Desligar o Sistema:* Registra reinicialização ou *shutdown* da máquina, bem como se o espaço para log de Security está cheio.
- *Controle de Processos:* Informação sobre o controle de processos do NT, como início e término, objetos acessados e outros.

Ao ligar a auditoria dos itens Controle de Processos e Uso dos Direitos do Usuário você estará gerando uma enorme quantidade de registros em seu log de segurança. Portanto deixe-os desligados e ligue a auditoria para os demais, esta informação pode ser crucial na detecção de um ataque ou de uma violação de segurança.

Algumas vulnerabilidades do Windows NT/2000

O problema principal para os Administradores de Rede é não deixar que um intruso consiga atingir os privilégios do super-usuário(no caso do NT, o administrador). Por isso a maior parte das vulnerabilidades descobertas são visando o status do super-usuário. Assim ele teria como realizar tudo dentro da máquina.

Vamos relatar algumas vulnerabilidades que ameaçam a segurança de um sistema com o Windows NT/2000.

Ataques de número de seqüência

Atinge todas as versões do Windows NT, e chega a ser de uma classe grave a critica até pelo fato de não haver solução ainda. Consiste no fato da adivinhação de um seqüência de portas abertas no protocolo TCP através de um programa de scaner de portas, isso dá ao invasor permissão completa para explorar todo o sistema de arquivos do micro.

A brecha do RDISK

O RDISK é um utilitário do Windows NT que permite a criação de discos de reparo de emergência. Para o administrador do sistema isso é muito importante, mas o RDISK é uma enorme brecha de segurança, pois ele faz um *dump* (levantamento) de todas as informações de segurança no diretório "C:\WINNT\REPAIR", daí se o atacante conseguir *crackear* a senha do sistema, em questão de horas a segurança da sua rede em horas estará 100% comprometida.

Mas a solução para isso é simples, após a criação do disco de reparo a administrador do sistema deve deletar o diretório acima citado, uma ação simples que passa a resolver um grande problema.

Novell Netware

Para se manter a integridade dos dados em uma rede local, *Netware*, precisamos desenvolver uma estratégia de segurança. Para isso usamos quatro níveis de segurança de servidor de arquivos disponíveis, que são:

- Segurança de conexão e senha;
- Segurança de consórcio;
- Segurança de diretórios;
- Segurança de atributos de arquivos e diretórios.

Segurança de conexão e senha:

Para que consigamos desenvolver uma estratégia de Segurança de Rede, precisamos estar *até*ntos no planejamento, e em todos os detalhes, pois se não for feito uma boa estratégia de planejamento, certamente ocorrerão problemas devido à falhas na segurança.

Existem 2 tipos de Segurança de Rede:

- *Restrições à usuários:* As restrições de usuário limitam o acesso a certos tipos de funções na rede.
- *Restrições de diretório de arquivos:* As restrições de arquivos limitam o acesso à dados específicos.

Restrições de usuário:

Primeiro nível de segurança de rede. Ele determina que a proteção seja executada por meio de uma senha, e o usuário só terá acesso à rede, mediante validação da mesma. Além disso, podemos impedir que um usuário se conecte à rede através de várias estações de trabalho, limitando o número de conexões concorrentes. Caso o usuário tente se conectar a partir de mais de uma estação ao mesmo tempo, aparecerá para ele uma

mensagem de erro, indicando que o usuário já está conectado, então, o acesso à rede será negado.

Outra forma de restrição dos usuários, é fazer com que o Netware monitore o número de senhas incorretas, informadas por um usuário, estabelecendo assim um limite. Caso esse limite seja excedido, o acesso do usuário será bloqueado.

Podemos também fazer com que o usuário somente possa acessar à rede em um determinado horário. Esse tipo de restrição, é muito utilizado para fins de manutenção geral, onde pode-se eliminar todas as conexões ativas, e bloquear conexões para que a manutenção do sistema possa ser feita naquele horário.

Observação: Apenas o supervisor da rede pode executar esses tipos de restrições de segurança.

Restrições de diretório e arquivo:

As restrições de diretório e arquivo, como o próprio nome já diz, limitam os direitos que os usuários tem de acessar diretórios, ou arquivos específicos, podendo ser atribuídos direitos diferentes a vários su*bbanco de dados*iretórios. Para su*bbanco de dados*iretórios que contenham sistema operacional, utilitários e programas, podemos conceder todos os direitos, a não ser o de procedências e eliminação, evitando assim, a modificação das estruturas de diretórios, ou remoção de um arquivo de programa.

Outra forma de assegurar a integridade, é o compartilhamento (*Shareable*) dos arquivos ou diretórios como somente leitura (*Read Only*).

Segurança de consórcio:

A Segurança de Consórcio, é o segundo nível de segurança do Netware. Neste podemos atribuir privilégios à usuários (e grupos de usuários) para trabalharem em diretórios, podendo ser concedidos oito direitos de consórcio à usuários. São eles:

- Leitura;

- Gravação;
- Abertura;
- Criação;
- Eliminação;
- Procedência;
- Pesquisa;
- Modificação.

Os direitos podem ser concedidos à usuários individuais, ou a todos usuários de um mesmo grupo.

Esses direitos também podem ser atribuídos, direta ou indiretamente através do uso de equivalências de segurança. A equivalência de segurança permite que o supervisor conceda a um usuário, ou a um grupo, os mesmos direitos de consórcio que concedidos a um outro usuário, ou grupo.

Somente um supervisor pode atribuir direitos de consórcio a um usuário.

Segurança de diretório:

O terceiro nível de segurança do Netware, é a segurança de diretório. Esse tipo de segurança está em um nível inferior no esquema Netware, porque ele possui precedência sobre os direitos de consórcio. Se for modificada a máscara de diretórios máximos (falada à seguir) associada com um su*bbanco de dados*iretório, você pode impedir que os usuários da rede exerçam alguns de seus direitos de consórcio.

Máscara de diretórios máximos:

A máscara de diretórios máximos contém os mesmos oito privilégios que podem ser atribuídos como direito de consórcio a um usuário. Eliminando direitos da máscara de direitos máximos, os direitos de consórcio podem ser cancelados.

Exemplo: Caso o direito de criação seja retirado da máscara de diretórios máximos do su*bbanco de dados*iretório PROGRAMS, ninguém pode criar um arquivo nesse mesmo su*bbanco de dados*iretório, independente dos direitos de consórcio do usuário. A máscara de direitos máximos sempre tem precedência sobre os direitos de consórcio. Uma vez que um direito tenha sido retirado da máscara de direitos máximos, somente um supervisor de sistema pode realizar a função eliminada.

Direitos efetivos:

Os direitos efetivos são determinados pela combinação dos direitos de consórcio do usuário e dos direitos de diretório.

Segurança de atributos de arquivos e diretórios:

A segurança de atributos de arquivos e diretórios é o quarto nível de segurança do Netware. Os atributos de arquivo e diretório tem precedência sobre até mesmo os direitos efetivos de um diretório.

Principais atributos de segurança de arquivo relacionados à segurança de rede:

Os principais atributos de arquivo no Netwarre são classificados como partilháveis (*shareabl*"), não partilháveis (*nonshareable*), leitura e gravação (*read-write*), e somente leitura (*read only*), onde suas funções podemos observar na tabela abaixo:

ATRIBUTO	FUNÇÃO
Partilháveis (Shareable)	Com direitos efetivos adequados, mais de um usuário pode ler o arquivo ao mesmo tempo.
Não-partilhável (Nonshareable)	Com direitos efetivos adequados, somente um usuário de cada vez pode ler o

	arquivo.
Leitura-gravação (Read-Write)	Com direitos efetivos adequados, um usuário pode ler, gravar, eliminar ou trocar o nome do arquivo.
Somente leitura (Read Only)	Com direitos efetivos adequados, um usuário pode ler o arquivo.

Quando são criados novos arquivos no Netware, são dados a ele atributos do tipo não compartilháveis e leitura-gravação. Esses atributos, permitem que apenas um usuário acesse e manipule o arquivo, considerando que esses usuários tenham direitos efetivos adequados.

Atributos de diretório:

A concessão de atributos à diretórios, é feita do mesmo modo que na consessão de atributos e arquivos e são classificados como escondido (*hidden*) e *privaté* (privativo), onde suas funções podemos observar na tabela abaixo:

ATRIBUTO	FUNÇÃO
Escondido (Hidden)	Tira o diretório de vista durante uma listagem de diretório, mas não impede que os usuários acessem o mesmo.
Privativo (Priv*até*)	Permite que os usuários vejam o diretório durante uma listagem de diretório, mas não o seu conteúdo.

Importante: Quando é concedido direito de consórcio a um usuário, em um diretório, ele automaticamente adquire os mesmos direitos em qualquer su*bbanco de dados*iretório, a não ser que haja um caso com determinada restrição.

CAPÍTULO IV - SEGURANÇA NA *INTERNET*

Considerações Iniciais

O aumento no número de usuários na rede *Internet* trouxe a preocupação com a segurança das informações, preocupação esta que cresce na mesma ou que sá em proporções maiores que o crescimento da própria rede.

Veremos neste capítulo alguns detalhes relacionados a segurança na *Internet*

Perigos numa conexão sem proteção adequada

Com o avanço tecnológico, principalmente nas áreas de informática, componentes eletrônicos e comunicação, houve a possibilidade da criação de uma grande rede de computadores, hoje conhecida como *Internet*.

Através da história constatamos que todo conhecimento humano pode ser usado tanto para o bem como para o mal.

Na informática também não é diferente, vimos freqüentemente serem noticiados na mídia sobre sistemas invadidos por pessoas com avançados conhecimento na área de informática, conhecidos como *Hackers*.

Esses especialistas se utilizam de falhas existentes nos sistemas operacionais e através de diversos mecanismos como FTP, TELNET, TROJANS, etc., conseguem invadir servidores e até micros pessoais.

A seguir falaremos sobre os principais protocolos de rede. Citaremos também os programas mais utilizados para invasão e os perigos que eles nos expõem, as portas utilizadas para invasão, sugestões para proteção.

Protocolos

TCP/IP

TCP/IP é o nome que se dá a toda a família de protocolos utilizados pela *Internet*. Esta família de protocolos foi desenvolvida pela DARPA (*Defense Advanced Research Project Agency*) no Departamento de defesa dos Estados Unidos.

Este conjunto de protocolos foi desenvolvido para permitir aos computadores compartilharem recursos numa rede. Toda a família de protocolos incluem um conjunto de padrões que especificam os detalhes de como comunicar computadores, assim como também convenções para interconectar redes e rotear o tráfego.

Mas ao contrário do que acontece na imprensa, o nome completo raramente é usado. O TCP e o IP são protocolos individuais que podem ser discutidos de modo isolado, mas eles não são os únicos protocolos que compõem essa família. Pode acontecer de um usuário do TCP/IP não utilizar o protocolo TCP propriamente dito, mas sim alguns protocolos da família. A utilização do TCP/IP nessa situação não deixa de ser apropriada porque o nome se aplica de modo genérico ao uso de qualquer protocolo da família TCP/IP.

Alguns Protocolos da família TCP

- ARP: (Address Resolution Protocol)
- ICMP: (*Internet* Control Message Protocol)
- UDP: (User Datagram Protocol)
- RIP: (Routing Information Protocol)
- HTTP: (Hypertext Transfer Protocol)
- NNTP: (Network News Transfer Protocol)
- SMTP: (Simple Mail Transfer Protocol)

- SNMP: (Simple Network Management Protocol)
- FTP: (File Transfer Protocol)
- TFTP: (Trivial File Transfer Protocol)
- INETPhone: (Telephone Services on *Internet*)
- IRC: (*Internet* Relay Chat)
- RPC: (Remote Procedure Call)
- NFS: (Network File System)
- DNS: (Domain Name System)

Talvez seja difícil lembrar todos esses acrônimos, até porque alguns também são utilizados por outros protocolos (por exemplo o protocolo RIP da família Novell, ou o IPX, é diferente do RIP da família TCP/IP).

Uma visão resumida do Protocolo.

Alguma transferência se inicia com um pedido de leitura ou escrita de um arquivo, o qual também serve para pedir uma conexão. Se o servidor reconhece o pedido, a conexão é aberta e o arquivo é enviado num bloco de tamanho fixo de 512 bytes. Cada pacote de dados contém um bloco de dados e deve ser reconhecido por um pacote de acknowledgment antes que o próximo pacote possa ser enviado. Um pacote de dados menor que 512 bytes sinaliza o termino de uma transferência.

Se um pacote consegue se perder na rede, o receptor indicara *time-out* e poderá retransmitir seu último pacote (o qual pode ser dados ou um reconhecimento). Isto motiva ao transmissor do pacote perdido a retransmitir o pacote perdido. O transmissor tem que guardar apenas um pacote para retransmissão, desde cada passo de reconhecimento garante que todos os pacotes mais anteriores tenham sido recebidos.

Muitos erros são causados pelo termino da conexão. Um erro é sinalizado enviando um pacote de erro. Este pacote não é reconhecido nem retransmitido (ie, um servidor TFTP

ou usuário pode terminar depois enviando uma mensagem de erro) assim o outro terminal da conexão não deve recebe-lo. Portanto os *time-out* são usados para detectar tais terminais quando o pacote de erro foi perdido.

Protocolo IP

O protocolo IP define mecanismos de expedição de pacotes sem conexão. IP define três pontos importantes:

- A unidade básica de dados a ser transferida na *Internet*.
- O software de IP executa a função de roteamento, escolhendo um caminho sobre o qual os dados serão enviados.
- Incluir um conjunto de regras que envolvem a idéia da expedição de pacotes não confiáveis. Estas regras indicam como os *hosts* ou *gatéways* poderiam processar os pacotes; como e quando as mensagens de erros poderiam ser geradas; e as condições em que os pacotes podem ser descartados.

Tipos de protocolos TCP

DNS

O DNS (*Domain Name System*) é um esquema de gerenciamento de nomes, hierárquico e distribuído. O DNS define a sintaxe dos nome usados na *Internet*, regras para delegação de autoridade na definição de nomes, um b*banco de dados* distribuído que associa nomes a atributos (entre eles o endereço IP) e um algoritmo distribuído para mapear nomes em endereços.

As aplicações normalmente utilizam um endereço IP de 32 bits no sentido de abrir uma conexão ou enviar um datagrama IP. Entretanto, os usuários preferem identificar as máquinas através de nomes ao invés de números. Assim e necessário um b*banco de dados* que permita a uma aplicação encontrar um endereço, dado que ela conhece o nome da máquina com a qual se deseja comunicar.

Um conjunto de servidores de nomes mantém o b*banco de dados* com os nomes e endereços das máquinas conectadas a *Internet*. Na realidade este é apenas um tipo de informação armazenada no *domain system* (sistema de domínios). Existem atualmente tantas instituições conectadas a *Internet* que seria impraticável exigir que elas notificassem uma autoridade central toda vez que uma máquina fosse instalada ou trocasse de lugar. Assim, a autoridade para atribuição de nomes e delegada a instituições individuais. Os servidores de nome formam uma árvore, correspondendo a estrutura institucional. Os nomes também adotam uma estrutura similar.

Exemplo: Um exemplo típico é o nome chupeta.jxh.xyz.br. Para encontrar seu endereço *Internet*, pode ser necessário o acesso a até quatro servidores de nomes. Inicialmente deve ser consultado um servidor central, denominado servidor raiz, para descobrir onde esta o servidor br. O servidor br é o responsável pela gerência dos nomes das instituições / empresas brasileiras ligadas a *Internet*.

O servidor raiz informa como resultado da consulta o endereço IP de vários servidores de nome para o nível br (pode existir mais de um servidor de nomes em cada nível, para garantir a continuidade da operação quando um deles para de funcionar). Um servidor do nível br pode então ser consultado, devolvendo o endereço IP do servidor xyz. De posse do endereço de um servidor xyz e possível solicitar que ele informe o endereço de um servidor jxh, quando, finalmente, pode-se consultar o servidor jxh sobre o endereço da máquina chupeta. O resultado final da busca e o endereço *Internet* correspondente ao nome chupeta.jxh.xyz.br.

Cada um dos níveis percorridos e referenciado como sendo um domínio. O nome completo chupeta.jxh.xyz.br é um nome de domínio.

Na maioria dos casos, não é necessário ter acesso a todos os domínios de um nome para encontrar o endereço correspondente, pois os servidores de nome muitas vezes possuem informações sobre mais de um nível de domínio o que elimina uma ou mais consultas. Além disso, as aplicações normalmente tem acesso ao DNS através de um processo local (servidor para as aplicações e um cliente DNS), que pode ser implementado de modo a guardar os últimos acessos feitos, e assim resolver a consulta em nível local.

Essa abordagem de acesso através de um processo local, simplifica e otimiza a tarefa das aplicações no que tange ao mapeamento de nomes em endereços, uma vez que elimina a necessidade de implementar, em todas as aplicações que fazem uso do DNS, o algoritmo de encaminhamento na árvore de domínios descrito anteriormente. O DNS não se limita a manter e gerência endereços *Internet*. Cada nome de domínio é um nó em um b*banco de dados*, que pode conter registros definindo várias propriedades. Por exemplo, o tipo da máquina e a lista de serviços fornecidos por ela. O DNS permite que seja definido um aliás (nome alternativo) para o nó. Também é possível utilizar o DNS para armazenar informações sobre usuários, listas de distribuição ou outros objetos.

O DNS é particularmente importante para o sistema de correio eletrônico. No DNS são definidos registros que identificam a máquina que manipula as correspondências relativas a um dado nome, identificado assim onde um determinado usuário recebe suas correspondências. O DNS pode ser usado também para definição de listas para distribuição de correspondências.

SMTP

O SMTP (*Simple Mail Transfer Protocol*) é o protocolo usado no sistema de correio eletrônico na arquitetura *Internet* TCP/IP. Um usuário, ao desejar enviar uma mensagem, utiliza o modulo interface com o usuário para compor a mensagem e solicita ao sistema de correio eletrônico que a entregue ao destinatário. Quando recebe a mensagem

do usuário, o sistema de correio eletrônico armazena uma cópia da mensagem em seu spool (área do dispositivo de armazenamento), junto com o horário do armazenamento e a identificação do remetente e do destinatário. A transferência da mensagem é executada por um processo em *background*, permitindo que o usuário remetente, após entregar a mensagem ao sistema de correio eletrônico, possa executar outras aplicações.

O processo de transferência de mensagens, executando em background, mapeia o nome da máquina de destino em seu endereço IP, e tenta estabelecer uma conexão TCP com o servidor de correio eletrônico da máquina de destino. Note que o processo de transferência atua como cliente do servidor do correio eletrônico. Se a conexão for estabelecida, o cliente envia uma cópia da mensagem para o servidor, que a armazena em seu *spool*. Caso a mensagem seja transferida com sucesso, o servidor avisa ao cliente que recebeu e armazenou uma cópia da mensagem. Quando recebe a confirmação do recebimento e armazenamento, o cliente retira a copia da mensagem que mantinha em seu *spool* local. Se a mensagem, por algum motivo, não for transmitida com sucesso, o cliente anota o horário da tentativa e suspende sua execução. Periodicamente o cliente acorda e verifica se existem mensagens a serem enviadas na área de *spool* e tenta transmiti-las. Se uma mensagem não for enviada por um período, por exemplo de dois dias, o serviço de correio eletrônico devolve a mensagem ao remetente, informando que não conseguiu transmiti-la.

Em geral, quando um usuário se conecta ao sistema, o sistema de correio eletrônico é ativado para verificar se existem mensagens na caixa postal do usuário. Se existirem, o sistema de correio eletrônico emite um aviso para o usuário que, quando achar conveniente, ativa o modulo de interface com o usuário para receber as correspondências.

Uma mensagem SMTP divide-se em duas partes: cabeçalho e corpo, separados por uma linha em branco. No cabeçalho são especificadas as informações necessárias para a

transferencia da mensagem. O cabeçalho é composto por linhas, que contem uma palavra-chave seguida de um valor. Por exemplo, identificação do remetente (palavra-chave "to:" seguida do seu endereço), identificação do destinatário, assunto da mensagem, etc... No corpo são transportadas as informações da mensagem propriamente dita.

O formato do texto é livre e as mensagens são transferidas no formato texto.

Os usuários do sistema de correio eletrônico são localizados através de um par de identificadores. Um deles especifica o nome da máquina de destino e o outro identifica caixa postal do usuário. Um remetente pode enviar simultaneamente várias cópias de uma mensagem, para diferentes destinatários utilizando o conceito de lista de distribuição (um nome que identifica um grupo de usuários). O formato dos endereços SMTP é o seguinte:

nome_local@nome_do_dominio

onde o nome_do_domínio identifica o domínio ao qual a máquina de destino pertence (esse endereço deve identificar um grupo de máquinas gerenciado por um servidor de correio eletrônico). O nome local identifica a caixa postal do destinatário.

O SMTP especifica como o sistema de correio eletrônico transfere mensagens de uma máquina para outra. O módulo interface com usuário e a forma como as mensagens são armazenadas não são definidos pelo SMTP. O sistema de correio eletrônico pode também ser utilizado por processos de aplicação para transmitir mensagens contendo textos.

CAPÍTULO V - VÍRUS

Introdução

Manter a segurança dos dados que trafegam numa rede de computadores é extremamente difícil, pois existem milhares e milhares de "programas intrusos" prontos para atacar o sistema e causar estragos irreparáveis. São os chamados vírus de computador, ou seja, programas potencialmente destrutivos feitos por alguém e colocados em circulação até atingir um computador através de arquivos infectados. São programas pequenos e simples que passam de programa para programa ou de disco para disco, se auto copiam fazendo ou não alterações em arquivos ou programas, sem conhecimento e sem autorização do usuário do computador infectado.

Com a popularização da *INTERNET* e das INTRANETS nas companhias, a proliferação dos vírus tomou dimensões ainda mais alarmantes, fazendo com que os vírus de computador entrassem na onda da globalização. Se há bem pouco tempo eles invadiam a maioria das máquinas basicamente pela inserção de disquetes infectados, agora eles atravessam fronteiras ancorados em qualquer mensagem de correio eletrônico que navega na *INTERNET*, ou arquivo para *download* contaminado.

O QUE SÃO VÍRUS DE PC?

Vírus de computador, são pequenos programas, cuja denominação é uma analogia aos vírus reais pelas seguintes características, presentes em todos os programas que podem ser chamados de vírus:

- Eles são muito pequenos, entre algumas centenas de bytes até alguns Kbytes;

- Eles se autocopiam parasitando outras entidades do computador, ou seja, possuem instruções para criarem autonomamente cópias de si mesmo atracadas em outros arquivos, à revelia do usuário.

É importante compreender que um vírus de computador, qualquer que ele seja, necessariamente precisa conter instruções para parasitar e criar cópias de si mesmo de forma autônoma e sem autorização específica (e normalmente sem conhecimento) do usuário para isso — eles são, portanto, auto-replicantes. Assim, programas como Trojans Horses e Worms não são vírus. Trojans Horses não se replicam e Worms não parasitam outras entidades para se replicarem — são entidades autônomas.

Os vírus de computador atingem os computadores à partir de "hospedeiros" diversos como programas, documentos, disquetes, arquivos de sistema etc., possuindo formas sistemáticas e específicas para sua multiplicação, contaminação e disseminação.

Um vírus, é um conjunto de instruções executadas pelo computador. Os vírus infectam à outros programas e aplicativos de forma que quando estes são executados, neste momento as instruções do vírus também são executadas sem que o usuário saiba. Os Vírus podem atingir os micros na inicialização do computador, execução de programas ou de macros.

A forma de disseminação pode ser feita através de disquetes, CDs, *downloads* de BBSs ou *Internet*. Quando um arquivo infectado é executado ao chegar ao destino, o vírus atinge à memória do seu computador, e passa a infectar outros arquivos, normalmente os chamados arquivos executáveis (extensão *.com, *.exe) e também algumas dll importantes para o sistema operacional.

Os vírus também podem infectar códigos executáveis localizados no setor de inicialização, que contém informações relacionadas à formatação do disco, dos diretórios e dos arquivos armazenados nele. Além disso, todo disco contém um pequeno programa

chamado de programa de boot (responsável pela inicialização do sistema), e que carrega os arquivos do sistema operacional (o DOS, por exemplo). Assim, um vírus pode estar escondido em qualquer disco, mesmo que este disco rígido ou disquete não seja de inicialização.

Outra forma de disseminação de vírus é através de macros. Alguns programas aplicativos habilitam seus arquivos de dados (documentos de texto ou planilhas, normalmente) à armazenarem instruções de macro. Alguns vírus são basicamente um conjunto de macros que permitem a sua auto-replicação a partir de um programa aplicativo infectado.

Um vírus se manifesta de diversas formas, mostrando mensagens, alterando determinados tipos de arquivos, diminuindo a performance do sistema, apagando arquivos, corrompendo a tabela de alocação de arquivos (FAT), ou mesmo apagando todo o disco rígido.

Uma boa parte dos vírus não tem por objetivo provocar danos reais ao seu computador. Podem não fazer nada além de apresentar mensagens em um determinado dia e ser tão inofensivos como o vírus Brain, que somente altera o label (rótulo) dos disquetes infectados.

Do lado oposto temos vírus intencionalmente destrutivos, corrompendo arquivos específicos, setores do disco, a Tabela de Alocação de Arquivos (*FAT – File Alocation Table*) ou o Registro Mestre de Inicialização (*MBR – Master Boot Record*).

Entretanto, muitos vírus que causam danos não o fazem intencionalmente. Muitas vezes são conseqüências de erros de programação, chamados *bugs*.

Um vírus maligno pode provocar:

- Erros na hora de execução de um programa;
- Baixa de memória;

- Lentidão para entrar em programas;
- Danificação de dados;
- Danificação de drives;
- Formatação indesejada do HD;
- Alocação desnecessária da memória do computador

É dificil termos um número exato dos tipos de vírus, porque não existe um consenso entre os pesquisadores em relação à classificação e denominação dos vírus conhecidos — quase todos os vírus de computador possuem mais de uma denominação (chamadas variantes), e literalmente novos vírus surgem a cada dia, sendo que muitos deles são apenas vírus já existentes com pequenas modificações e edições. Mas apesar das estimativas dos especialistas indicarem um enorme número de espécies conhecidas (mais de 20.000), com um incremento de cerca de uma centena de vírus novos ao mês, apenas uma pequena parcela é a responsável por quase totalidade (estima-se cerca de 98%) dos registros de infecções no mundo.

Prevenção

Quando o computador está infectado, é comum o aparecimento dos seguintes sintomas: mensagens indevidas, músicas, ruídos ou figuras e desenhos, alteração no tamanho de algum arquivo, redução da quantidade de memória disponível, atividades demoradas no disco rígido. Para um nível maior de certeza e segurança, é essencial manter-se um antivírus sempre atualizado no computador. Para evitar problemas, sempre é bom checar disquetes desconhecidos antes de inseri-lo no computador, bem como arquivos recebido via *Internet*.

É impossível adquirir vírus por meio de uma mensagem de correio eletrônico, a não ser que nela exista um arquivo contaminado anexado e que tal arquivo seja aberto num computador sem proteção de um antivírus adequado. Isso porque o vírus não pode viajar

na mensagem, que é formada apenas por letras e números, precisando sempre de um programa ou de um documento capaz de conter macros.

Um vírus, pode atacar o programa de antivírus instalado no seu computador, portanto tenha sempre à mão um disco de emergência com a inicialização do seu sistema operacional e um antivírus que possa ser rodado a partir dele.

É interessante também fazer cópias de segurança (*backups*) dos arquivos de um computador, pois essas são essenciais na manutenção integra dos dados.

Outra medida de precaução diz respeito aos programas piratas (cópias ilegais de programas de computador). Não deve-se confiar muito neles uma vez que sua procedência não é tão segura quanto a de um software legal.

Programas anti-vírus

Programas anti-vírus, são programas utilizados para detectar vírus num computador ou disquete. A maioria usa método simples de procura por uma sequência de bytes que constituem o programa vírus. Desde que alguém tenha detectado e analisado a sequência de bytes de um vírus, é possível escrever um programa que procura por essa sequência. Se existe algo parecido, o programa antivírus anuncia que encontrou um vírus. O antivírus, por sua vez, funciona como uma vacina dotada de um b*banco de dados* que cataloga milhares de vírus conhecidos. Quando o computador é ligado ou quando o usuário deseja examinar algum programa suspeito, ele varre o disco rígido em busca desses sinais de invasores.

Quando um possível vírus é detectado, o antivírus parte para o extermínio. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes, a única saída é substituir o arquivo infectado pelo mesmo arquivo do disco de emergência do software original, ou de outro computador com programas e sistema operacional idênticos ao infectado. Dependendo do vírus e das proporções dos

danos ocasionados pela virose, fica praticamente impossível a restauração do ambiente operacional.

Nenhum antivírus, no entanto, é 100% infalível, dentre os mais eficientes, destaca-se o VirusScan 4.5 da McAfee. Esse detecta e remove mais vírus que os outros softwares. Além disso, oferece muito mais recursos do que outros softwares, como filtro para arquivos vindos da *Internet*.

- *Tecnologia Push:* atualiza a lista de vírus. Ao conectar-se à *Internet*, o micro aciona o software Backweb, que busca automaticamente novas versões da lista de vírus no site da McAfee sem a necessidade do usuário fazer *dowloads* manuais;
- *ScreenScan:* varre o disco rígido enquanto o micro está ocioso. Funciona da seguinte maneira: toda vez que o screen saver é acionado, o VirusScan entra em ação. Além de não atrapallar a rotina do usuário, evita a queda de desempenho do PC.

A seguir uma lista dos principais antivírus do mercado e suas respectivas funções especiais:

ANTIVÍRUS	**VERIFICA ARQUIVOS**		
	DURANTE DOWNLOADS	**ANEXADOS EM E-MAILS**	**COMPACTADOS**
	COMPACTADOS OU NÃO	**COMPACTADOS OU NÃO**	**DOS / WINDOWS 95**
Dr. Salomons 7.73	Não/Sim	Não/Sim	Não/Não
F-Prot 3.01	Não/Sim	Não/Sim	Não/Não
Inoculan 5.0	Sim/Sim	Sim/Sim	Sim/Sim
Imune Vírus II 2.0	Não/Sim	Não/Sim	Sim/Não
Norton AntiVírus 6.0	Sim/Sim	Não/Sim	Não/Não
PC-cillin 97 2.10	Sim/Sim	Sim/Sim	Sim/Sim

Sweep	Não/Sim	Não/Sim	Não/Não
TBAV	Não/Sim	Não/Sim	Não/Não
VirusScan 4.5	Não/Sim	Não/Sim	Sim/Não

Classificação dos vírus:

As classificação dos vírus, são definidas de uma forma geral, pelos alvos de infecção e disseminação. Assim, podemos classifica-los em três classes:

- *Vírus de arquivos ou programas:* Os vírus de arquivos ou programas, visam primeiramente os arquivos executáveis de programas e aplicativos;
- *Vírus de boot (inicialização) ou de sistema:* Os vírus de boot, visam instruções executáveis específicas existentes nos setores de inicialização dos discos rígidos ou flexíveis.
- *Vírus de macro:* Os vírus de macro, visam programas que suportem documentos e arquivos com macros (como, por exemplo, o Word e Excel da Microsoft).

Costuma-se denominar de vírus multipartites ou bimodais aqueles que infectam tanto arquivos executáveis como áreas de inicialização de discos.

Agora iremos falar um pouco mais detalhadamente sobre sua classificação:

Vírus de Arquivos ou de Programas

Os vírus de Arquivos ou de Programas, infectam basicamente arquivos executáveis que possuem a extensão .com ou .exe, mas podem também infectar outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .sys, .ovl, .ovy, .prg, .mnu, .bin, .drv, etc...

Quando executamos um programa (que consiste normalmente de um ou mais arquivos executáveis), ele é carregado na memória do computador para ser processado. Se ele estiver infectado, os códigos viróticos também são processados. Após à execução,

normalmente o programa é liberado da memória, a não ser que seja um programa residente em memória (TSR)?. A maioria dos vírus de arquivo, contudo, pode permanecer residente em memória.

Quando um vírus de arquivo não continua na memória do sistema após sua execução ele é chamado de vírus de arquivo de ação direta. Um vírus de ação direta funciona da seguinte forma: A cada vez que um arquivo infectado é executado, ele seleciona um ou mais programas para contaminar. Já um vírus residente, permanece escondido em algum lugar na memória na primeira vez que um programa infectado é executado. Da memória do computador passa a infectar os demais programas que sejam executados, ampliando progressivamente a contaminação.

Vírus de Sistema ou Inicialização (boot)

Os vírus de Sistema ou Inicialização, infectam códigos executáveis localizados em certas áreas de sistema do disco. Todo drive de disco, seja disco rígido ou flexível, contém um setor de inicialização, e reservam uma parte dele para informações relacionadas à sua formatação, dos diretórios e dos arquivos armazenados, além de um pequeno programa chamado de programa de *boot*, responsável pela inicialização do sistema operacional. É esse pequeno programa que vai dizer ao computador em que parte do disco estão os demais arquivos necessários para a inicialização do sistema.

Todos os discos possuem área de inicialização (*boot*), mesmo que o disco não seja de inicialização. Nesse caso, o setor de *boot* retorna ao usuário uma mensagem do tipo "o disco não tem sistema" nos seguintes casos:

- Leitura de um disquete sem sistema durante a inicialização do computador.
- Quando o disco rígido principal (mestre) não possui sistema operacional.

Portanto, um vírus de sistema pode se esconder em qualquer disco ou disquete, mesmo que ele não seja destinado à inicialização do sistema. Esses vírus visam se

disseminar através de disquetes que são levados de um PC ao outro, e que por ventura possam ser esquecidos no drive durante a inicialização. Quando um sistema é inicializado, normalmente ele procura um disquete no drive A antes de inicializar pelo drive C. Caso exista um disquete infectado, resultará na execução do vírus, sua residência na memória e contaminação dos discos acessados por esse PC.

Vírus de Macro

Os Vírus de Macro, constituem uma c*até*goria relativamente nova de vírus. As primeiras contaminações trouxeram capacidades inéditas para o mundo dos vírus. Os macrovírus, ao contrário dos tradicionais vírus de arquivos executáveis e de boot, podem atacar o mesmo programa em mais de um tipo de plataforma (Windows 3x, Windows 98 e Mac OS, por exemplo) e se disseminam em arquivos de dados que suportem macros do programa aplicativo. Pela facilidade de manuseio na criação e edição destes tipos de vírus, eles já são a família mais numerosa.

Muitas pessoas tem uma visão errada dos macrovírus, pois crêem que eles sejam feitos da mesma forma que os vírus convencionais, ou seja, em linguagem de baixo nível, como o Assembly. Porém eles são muito diferentes, tanto que as formas de detecção antigas são inúteis para detecta-los, já que os Antivírus anteriores a 1996 não foram programados para verificar instruções em linguagem de macro, muito menos avaliar sua periculosidade.

Os macrovírus se utilizam das características de funções "macro", comuns em programas de processamento de texto (Word) e planilhas de cálculo (Excel). Ao contrário dos vírus até então existentes, que se limitavam à arquivos executáveis ou afins e áreas de boot, os macrovírus infectam e disseminam-se por certos tipos de arquivos de dados. Isso permite uma disseminação muito mais acentuada pois, documentos e dados são trocados com frequência entre os usuários, ao contrário do que ocorre com programas propriamente

ditos. As chances de contaminação através de dados e documentos infectados também são bem maiores se comparadas às chances de se inicializar o computador com um disquete infectado no drive. Além disso, os macrovírus constituem a primeira c*até*goria de vírus multiplataforma, não se limitando à PCs, podendo potencialmente infectar também outras plataformas que usem o mesmo programa, como o Macintosh, por exemplo.

Estratégias de Prevenção

Não existem computadores imunes a vírus, e não existem programas que possam nos dar 100% de proteção — novos vírus estão sempre surgindo e eles são projetados para burlar os antivírus. Arquivos que não são atualmente checados por antivírus hoje podem ser hospedeiros de vírus amanhã. Por exemplo, até o surgimento dos macrovírus, os antivírus normalmente não verificavam arquivos *.doc e mesmo quando habilitadas a verificar, não eram programados para descobrir macros viróticas, o que permitiu que inúmeros computadores devidamente protegidos por antivírus se infectassem e se tornassem disseminadores de macrovírus.

Uma estratégia preventiva contra vírus de computador deve ser feito preferencialmente em dois níveis:

- *Prevenção de infecção:* barreiras de checagem e monitores residentes em memória são as linhas de defesa para evitar a contaminação do PC.
- *Prevenção contra danos:* disquetes de inicialização, disquetes de emergência criados por softwares antivírus e *backups* para neutralizar ou minimizar os danos quando o computador já está infectado.

A prevenção de infecção visa evitar que o micro seja infectado de uma forma geral. Raramente um vírus passará por essa barreira de defesa quando ela for bem realizada, a não ser um novo vírus que utilize novas técnicas ou que o antivírus utilizado esteja desatualizado.

A prevenção contra danos, visa um mecanismo de defesa para que caso um vírus ultrapasse a barreira de proteção, danifique o mínimo possível.

Prevenção de Infecção

Alguns procedimentos de prevenção são suficientes para fechar o cerco ao eventual primeiro contato do vírus com o seu PC. O essencial aqui é ter um antivírus atualizado e, opcionalmente, um monitor antivírus residente em memória.

Com um scanner antivírus devemos tomar os seguintes procedimentos:

- Fazer um scan inicial por todos os arquivos visados por vírus do seu disco rígido e de preferência em todos os seus disquetes, mesmo aqueles sem dados gravados. O scanner antivírus deverá ser ajustado para checar os setores de boot, MBR e memória do computador.
- Ajustar o antivírus para scanear os setores de boot, MBR e memória do computador em toda inicialização é uma boa medida preventiva, para bloquear vírus de sistema que venham a infectar algum arquivo de inicialização.
    1. detector, se possuir um checksummer (ou "vacinador"), deve ser habilitado para "vacinar" todos os tipos de arquivos visados pelos vírus. É desnecessário vacinar todos os arquivos do disco, basta vacinar apenas os arquivos visados pelos vírus (arquivos de dados simples, como txt, html, som e imagem, por exemplo, não são infectáveis).
    2. detector deverá ser utilizado toda vez que um disquete não examinado for aberto. Não permita a leitura de disquetes suspeitos antes de examina-los.
- Travar fisicamente contra gravação todos o disquetes com programas de instalação, *backup-us* e *drives*.
- Habilitar a checagem automática de arquivos vindos de *download* pela *Internet*.

- Se não possuir checagem automática de arquivos vindos da *Internet*, cheque sempre os arquivos potencialmente infectáveis, principlamente os arquivos *.doc, *.xls e *.exe.
- Não abrir ou executar arquivos suspeitos ou de origem não confiável obtidos via *Internet* ou BBS, ou mesmo atachado em e-mails sem serem examinados.
- Atualizar constantemente o antivírus.
- Após uma atualização, checar todo o HD.

Os disquetes de emergência são feitos pelos antivírus e não devem ser dispensados.

Um antivírus ajustado para scanear os setores de *boot*, MBR e memória do computador em toda inicialização, garantirá que um vírus detectado não se dissemine caso ele consiga atingir alguma dessas áreas do computador. O monitor residente em memória também alerta imediatamente tentativa de residência em memória por vírus ou alteração de arquivos protegidos.

Um vírus sempre objetiva se disseminar o máximo possível até ser descoberto ou causar um evento fatal para o qual foi construído, como, por exemplo, apagar todo disco rígido. Entretanto, é comum o aparecimento de alguns sintomas perceptíveis, mesmo sem o uso de antivírus, quando o computador está infectado. Usualmente, tais sintomas são alterações na performance do sistema e, principalmente, alteração no tamanho dos arquivos infectados. Uma redução na quantidade de memória disponível pode também ser um importante indicador de virose. Atividades demoradas no disco rígido e outros comportamentos suspeitos do seu hardware podem ser causados por vírus, mas também podem ser causadas por softwares genuínos, por programas inofensivos destinados à brincadeiras ou por falhas e panes do próprio hardware.

Outros sintomas de contaminação são propositalmente incluídos na programação dos vírus pelos próprios criadores, como: mensagens, músicas, ruídos ou figuras e

desenhos. Tais sintomas podem ser as provas definitivas de infecção, mas podem se tornar evidentes apenas quando a infecção já está alastrada pelo computador.

Quando constatado que um PC está infectado ou que possui alta suspeita de infecção, antes de mais nada, ele deve ser desligado e inicializado com um disco de emergência criado pelo antiírus.

Caso disponha desses, será praticamente o suficiente para resolver o problema desde que estejam atualizados.

É importante saber que os antivírus são produzidos para reparar os arquivos contaminados, entretanto nem sempre isso é possível. Além disso, o arquivo pode não ser corretamente reparado.

Quando um arquivo não pode ser reparado ou é mal reparado, ele pode e deve ser substituído por um mesmo arquivo "limpo" do software original ou de outro computador com programas e sistema operacional idênticos ao infectado.

CAPÍTULO VI – TROJAN

O que é Trojan?

Trojan, também conhecido como cavalo de tróia, é um formado por dois executáveis (Cliente e Servidor). O Cliente é utilizado para acessar o micro infectado pelo Servidor. O Servidor infecta um micro abrindo determinadas portas para acesso via rede *Internet*. Geralmente esses programas servidores ficam invisíveis depois de executados.

Mais conhecidos

Veremos abaixo alguns trojans mais utilizados:

Back Orifice

Back Orifice (orifício traseiro), além de ser pequeno (120Kb), camuflado — uma vez instalado, "desaparece" dentro de seu computador, sendo que o executável contendo o código pode ter qualquer nome, até mesmo um inocente readme.txt — é altamente letal. O programinha é pequeno e pode ser acoplado a qualquer executável, tal como um vírus. Uma vez executado, o Back Orifice apaga seus rastros do sistema e passa a servir requisições de qualquer um que queira conectar-se a sua máquina.

Como o Back Orifice funciona ?

O intruso precisa de dois arquivos e a *Internet*. Um dos arquivos, o programa servidor, deverá ser instalado em uma máquina que esteja rodando o Windows 95/98. O outro (programa cliente) acessa via *Internet* o programa servidor e faz o que bem entender com o computador do outro. Esse programa cliente está disponível tanto para Windows como para Unix. Obviamente, o servidor só roda em Windows 95/98. Ele especificamente não roda no Windows NT.

Lembre-se que o BO não é um vírus que se alastra pelas máquinas. Você não pode ser infectado pelo BO sem querer. O programa deve ser executado na sua máquina para que ela fique infectada.

O que o Back Orifice faz ?

Se não fosse pelo seu caráter malicioso, o BO poderia ser considerado um excelente programa para acesso e monitoramento remoto de um computador.

Suas proezas:

- Grava o conteúdo de sua tela em um arquivo.JPG
- Contém um servidor HTTP integrado, através do qual pode-se navegar pela sua árvore de diretórios.
- Possui capacidade para examinar tudo o que se passa na sua rede, podendo, desta forma, capturar todas as suas senhas e outras informações confidenciais que não foram enviadas criptografadas (você usa o servidor Web seguro para fazer compras na *Internet*, não é?).
- Monitora o seu teclado, guardando todas as letras que você digitou.
- Remaneja suas conexões, ou seja, se você possui um servidor web ou de FTP em sua máquina, a conexão pode ser redirecionada para outro endereço.
- Permite abrir uma janela DOS remotamente.
- Permite rodar um programa no computador da pessoa.

É transparente ao usuário. Ele não aparece em lugar nenhum do sistema, nem quando você tecla CTRL-ALT-DEL.

É seguro, as informações trocadas entre o servidor e o cliente são criptografadas com uma senha.

Perigoso: O invasor pode rebootar, travar a máquina infectada. Pode também fazer alterações no Registry.

Como ocorre a infecção ?

Só existem dois modos de o seu computador ser infectado: executando o programa servidor do BO e executando um programa que está infectado com o B.O.

***Até*nção:** o BO não infecta os outros programas do seu sistema. Essa infeção deve ser feita manualmente, usando outro programa disponível para isso. Uma vez instalado, ele não faz mais nada. Apenas responde requisições do programa cliente. Diante disso, podemos visualizar alguns casos em que você poderá ser atacado:

Você recebe um e-mail com um arquivo, solicitando que você o abra porque o programa "é legal" etc. Você roda o programa e, realmente, é muito interessante. No entanto, o programa automaticamente já infectou o seu computador com o Back Orifice.

Um "espírito de porco" sentou em cada uma das máquinas da sua rede de computadores e executou o BO.

Alguém acessou remotamente o seu diretório C:\Windows\Start Menu\StartUp (ou C:\Windows\Menu Iniciar\Inicializar) e copiou o programa servidor para lá. Como se sabe, a cada *boot* o Windows executa todos os programas que estão dentro desse diretório, incluindo o BO.

Você está infectado ?

O BO é relativamente fácil de detectar e remover. Existem duas saídas: ou você faz o trabalho sujo ou deixa para um programa fazê-lo.

Primeiro iremos descrever como remover manualmente: para você saber se está infectado ou não, clique com o botão direito no seu diretório do Windows (normalmente C:\Windows), escolha a opção "Localizar", clique em "Avançado" e no campo "Com texto" digite: Server: BO.

Se o BO estiver no sistema, irá aparecer um arquivo de aproximadamente 120Kb (o tamanho varia) e com um nome qualquer (provavelmente ".exe").

No exemplo, vemos o BO em ação: achamos o arquivo com o inocente nome LEIAME.TXT, que na verdade não é um arquivo texto, mas sim o programa servidor. Não tente remover esse arquivo ainda, você não irá conseguir.

Para remover faça o seguinte: Rode o programa RegEdit, através da opção Run do Start Menu. Abra o registro "KEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\RunServices" (clique duas vezes em HKEY_LOCAL_MACHINE, depois duas vezes em SOFTWARE, e assim por diante). No lado direito, deverá paracer uma série de programas que devem rodar quando o Windows é iniciado. Apague a linha que contém o arquivo. Agora reinicie o Windows e finalmente apague o arquivo que você encontrou. Pronto: o BO está fora da sua máquina!

Você também pode utilizar alguns programas já prontos para a remoção.

O AntiGen é um deles, faça o *download* do programa, rode e pronto. Seu sistema está limpo!

Certifique-se que ele realmente limpou o seu computador seguindo os passos descritos acima. Mais uma opção é o Back Orifice Eliminator.

Se você não quer depositar sua confiança em um programa desconhecido, acesse a página da Network Associ*até*s e faça o *download* do *upgrade* do Viruscan que detecta e remove o intruso.

A Microsoft enviou um *press-release* abordando a questão e dizendo que usuários que seguem os padrões de Segurança usuais não seriam afetados. Seguindo essa linha, aqui vão algumas dicas para minimizar o perigo de ser infectado:

- Seja mais cuidadoso com o compartilhamento de arquivos: jamais compartilhe o diretório C:\Windows.
- Nunca abra arquivos executáveis que venham por e-mail.

- Se você tiver que reinstalar algum programa, utilize o disquete/CD-ROM original ou uma cópia que você tenha certeza que não foi modificada.
- Se possível instale um firewall na sua rede.

NetBus

O NetBus é um cavalo de tróia (tem seu código escondido dentro de outro programa executável) que, assim como o Back Orifice, explora as falhas de segurança do Windows. Uma vez instalado no computador, permite que um usuário remoto não-autorizado tenha total controle sobre a máquina da vítima.

Detalhe: O NetBus, diferentemente do Back Orifice, funciona também no ambiente Windows NT.

Para se proteger do NetBus, valem algumas regras básicas, que devem ser seguidas por qualquer usuário de computador, esteja ele ou não conectado à *Internet* ou a uma rede local: Ter um software antivírus instalado e sempre atualizado, não abrir arquivos executáveis (.exe, por exemplo) de fontes não conhecidas, não abrir arquivo algum do disquete sem passar o antivírus.

Todos os meses, os fabricantes de antivírus colocam em seus sites atualizações das bibliotecas de vírus. O arquivo DAT 3110 do VirusScan 3.2.0, disponível para *download*, já detecta o intruso.

Mas é possível detectar o NetBus sem um programa antivírus. Proceda da seguinte maneira:

No menu INICIAR, clique em PROGRAMAS e depois em PROMPT do MS-DOS.

Na janela do MS-DOS, digite **netstat –an | find "12345"**

Caso o NetBus esteja hospedado na sua máquina, pode aparecer uma linha de comando com as seguintes características:

TCP 0.0.0.0:12345 0.0.0.0:0 LISTENING

O que fazer quando o NetBus for detectado ?

Existem programas escritos especialmente para remover cavalos de tróia, uma outra forma de remoção é recorrer ao próprio NetBus, que tem uma função de desinstalar (*uninstall*).

Conecte-se ao provedor de acesso.

Em INICIAR, EXECUTAR, digite WINIPCFG.

Anote o endereço IP informado.

Chame o NetBus, informe o endereço IP anotado e peça **"Server Admin"** e depois **"Remove Server"**.

***ATÉ*NÇÃO**: Esse recurso só funciona se o agressor que instalou o NetBus em sua máquina não tiver especificado uma senha. Se foi especificada uma senha, ela pode ser descoberta pelo Registry do Windows (em INICIAR, EXECUTAR, digite REGEDIT e verifique a chave **"HKEY_CURRENT_USER\PATCH\SETTINGS\ SERVERPWD"**, que contém a senha). Cuidado com modificações no REGISTRY, modificações erradas podem causar danos ao sistema.

Remoção Manual

O NetBus também pode ser removido manualmente. Em geral, esse recurso funciona mesmo que o NetBus tenha senha. Proceda da seguinte maneira:

Conecte-se ao provedor de acesso.

Em INICIAR, EXECUTAR, digite WINIPCFG.

Anote o endereço IP.

Em INICIAR, EXECUTAR, digite TELNET, seguido do endereço anotado mais 12345. (Exemplo: **telnet 200.300.100.1 12345**).

Digite **Password;1** ; dê enter.

Digite **RemoveServer;1** ; dê enter.

Pronto, seu computador está livre do NetBus.

Wincrash

O WinCrash é um programa dividido em duas partes, um Cliente e um Servidor... O Cliente é o programa que é utilizado para se conectar ao Servidor (SERVER.EXE) pela *Internet* ou por uma rede interna com protocolo TCP/IP. Para se conectar ao Servidor (server.exe) ele precisa estar rodando no computador. O Servidor é invisível, não aparecendo nem no CTRL+ALT+DEL (lista de processos visíveis rodando). Quando o Servidor é executado, ele se auto-instala no sistema, se executando toda vez que o Windows reiniciar... Para se conectar ao Servidor basta saber o IP. Os serviços funcionam através de pacotes encriptados, usando como chave o IP local e o IP remoto... A Interface do Cliente é simples e fácil de entender, até para quem não sabe Inglês, pois as descrições dos serviços estão em Português... O invasor usa o Cliente para operar o Servidor, tendo muito mais controle do que a própria pessoa que está em frente ao micro remoto (Servidor).

Portas mais utilizadas pelos Trojans

NOMES DOS TROJANS	PORTA UDP	PORTA TCP
Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash, FTP Trojan		21
Tiny Telnet Server		23
Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy, Kuang2, ProMail Trojan		25
Hackers Paradise, Agent 31, Masters Paradise		31
DeepThroat		41
DMSetup		58
Firehotcker		79

Executor		80
ProMail Trojan		110
JammerKillah		121
TCP Wrappers		421
Hackers Paradise		456
Rasmin		531
Ini-Killer, Phase Zero, Stealth Spy		555
Satanz Backdoor, Attack FTP		666
Dark Shadow		911
DeepThroat		999
Silencer, WebEx		1001
Doly Trojan		1011
Doly Trojan		1012
NetSpy		1024
Rasmin		1045
Xtreme		1090
Psyber Stream Server, Voice		1170
Ultors Trojan		1234
BackDoor-G, SubSeven		1243
VooDoo Doll		1245
BO DLL	1349	
FTP99CMP		1492
Shivka-Burka		1600
SpySender		1807
Shockrave		1981
BackDoor		1999
Trojan Cow		2001

Ripper		2023
Bugs		2115
Deep Throat, The Invasor		2140
Striker		2565
WinCrash		2583
Phineas Phucker		2801
WinCrash		3024
Masters Paradise		3129
Deep Throat, The Invasor		3150
Portal of Doom		3700
WinCrash		4092
File Nail		4567
ICQ Trojan		4590
Sockets de Troie, Bubbel, Back Door Setup		5000
Sockets de Troie, Back Door Setup		5001
Firehotcker		5321
Blade Runner		5400
Blade Runner		5401
Blade Runner		5402
ServeMe		5555
BO Facil		5556
BO Facil		5557
Robo-Hack		5569
WinCrash		5742
The Thing		6400
DeepThroat		6670
DeepThroat		6771

BackDoor-G, SubSeven		6776
Indoctrination		6939
G*até*Crasher, Priority		6969
Remote Grab		7000
NetMonitor		7300
NetMonitor		7301
NetMonitor		7306
NetMonitor		7307
NetMonitor		7308
ICKiller, BackDoor Setup		7789
Portal of Doom		9872
Portal of Doom		9873
Portal of Doom		9874
Portal of Doom		9875
iNi-Killer		9989
Portal of Doom		10067
Portal of Doom		10167
Acid Shivers		10520
Coma		10607
Senna Spy		11000
Progenic trojan		11223
Hack'99 KeyLogger		12223
GabanBus, NetBus, Pie Bill G*até*s, X-bill		12345
GabanBus, NetBus, X-bill		12346
Whack-a-mole		12361
Whack-a-mole		12362
WhackJob		12631

Senna Spy		13000
Priority		16969
Millennium		20001
NetBus 2 Pro		20034
GirlFriend		21544
Prosiak		22222
Evil FTP, Ugly FTP		23456
Delta	26274	
SubSeven (new)		27374
The Unexplained	29891	
AOL Trojan		30029
NetSphere		30100
NetSphere		30101
NetSphere		30102
Sockets de Troie		30303
Back Orifice Client, Baron Night, B02, Bo Facil		31337
BackFire, Back Orifice, DeepBO	31337	
NetSpy DK		31338
Back Orifice, DeepBO	31338	
NetSpy DK		31339
BOWhack		31666
Prosiak		33333
BigGluck, TN		34324
The Spy		40412
Masters Paradise, Agent 40421		40421
Masters Paradise		40422
Masters Paradise		40423

Masters Paradise		40426
Delta	47262	
Sockets de Troie		50505
Fore		50766
Remote Windows Shutdown		53001
School Bus		54321
DeepThroat		60000
Telecommando		61466
Devil		65000

Como se Protejer

Existem diversas maneiras de você proteger seu micro de uma provável invasão:

- Não deixe seu micro ser utilizado por pessoas estranhas, sem que você saiba o que estão fazendo. Existem internautas que quando conseguem acessar um micro alheio, instalam programas que facilitam a invasao;
- Utilize programas para bloquear o acesso a gravação de arquivos;
- Utilize um bom utilitário anti-virus;
- Existem programas no mercado que controla o acesso as portas acima mencionadas. Esses programas são conhecidos como *firewall*;
- Não execute arquivos com extensão.EXE recebidos junto com emails;
- Muito cuidado com joguinhos disponibilizados na *Internet*. Pode estar contaminados com Trojans;
- Não receba arquivos executáveis enviados nas salas de chat. Muitos internautas mal intencionados enviam arquivos servidores de trojans com nomes disfarçados. Por exemplo: fotos.exe, xr*até*d.exe, sound.exe,etc.

CAPÍTULO VII – HACKERS

Geralmente quando falamos de *hackers* ouvimos falar daquelas pessoas que invadiram um *site*, que roubaram um monte de números de cartões de crédito e fizeram danos à várias empresas (mais a frente veremos que é um erro chamar essas pessoas de *hackers* pois dentro do submundo virtual essas "tribos" tem sua própria divisão).

O termo *hacker* era usado, originalmente, para designar qualquer pessoa que fosse especialista em qualquer área, mas foi na década de 80 que o termo ficou mais ligado com a computação, devido a filmes que falavam em pessoas especialistas em computação que invadiam sistemas alheios, sem a autorização dos donos. Isso popularizou o termo mas não foi o inicio de tudo, pois já existiam "*hackers* da informática, que eram pessoas que trabalhavam a fundo em pesquisas, mas também existiam aqueles garotos que gastam noites em claro só para descobrir uma falha em um sistema e estuda-la para se aproveitar (bem ou mal) dela.

A divisão do sub-mundo

Dentro do submundo dos *hackers* a divisão é bem simples, ou você tem conhecimentos aprofundados em um determinado assunto (de preferência pouco explorado) ou você não é conhecido dentro do submundo, ou seja, ou você se encaixa no grupo dos verdadeiros gênios da computação, ou você é praticamente ignorado.

Dentro do pequeno grupo dos *hackers* podemos dar importância a três grupos distintos:

- *Hackers:* São pessoas com grande facilidade de aprender técnicas variadas que o levarão a fazer o que quiser com um computador.

Devido ao seu profundo conhecimento, dessas técnicas, ela tem a capacidade de chegar as falhas dos sistemas que ele sabe que existem, pois um sistema não é completamente livre de erros.

- *Cracker:* Possui o mesmo nível de conhecimento de *hacker*, mais com uma diferença, para ele não importa somente entrar em sistemas através do descobrimento de uma falha, da quebra de uma senha; ele precisa "aparecer", deixar um rastro de sua presença, como a destruição de partes de um sistema, o roubo de dados e até mesmo recados mal-educados através de substituição de páginas na *Internet*. São atribuídos também aos *crackers* os programas que retiram as travas de software e que alteram suas características principais, tudo relacionado à pirataria de software.
- *Phreaker:* É o *hacker* da telefonia. Onde entre suas principais atividades são as ligações gratuitas, reprogramação de centrais telefônicas, instalação de escutas (fazendo o *phreaker* escutar ligações alheias) etc...

O conhecimento de um *phreaker* é muito útil para pessoas mal-intencionadas, pois além de permitir que uma invasão de sistema se origine de provedores de acesso de outros países, seus conhecimentos também permitem que ele não seja rastreado e que ele coloque forje *até* um possível culpado.

Além destes grupos acima citados, existem inúmeras categorias de "não-*hackers*", de onde surgem os pretendentes a *hackers*. Tais como:

- *Lamers:* É aquela pessoa que lê tudo sobre *hackers* tentando ser um deles. E acaba sendo insultado pelos *hackers* sendo chamado de "novato".
- *Wannabe:* "É o principiante que aprendeu a usar algumas receitas de bolo (programas já prontos para descobrir senhas ou invadir sistemas), entrou em um provedor de fundo de quintal e já acha que vai conseguir entrar nos computadores da NASA" (Revista *Internet* World – Numero 23 – Julho de 1997).

- *Larva:* Esse já esta quase lá. Já consegue desenvolver suas próprias técnicas para atacar sistemas.
- *Arackers:* Maioria absoluta no submundo cibernético, são os "*hackers*-de-araque", parecem ser ousados e muito espertos no que se trata da tecnologia, planejam ataques, fazem reuniões importantes mas acabam fazendo menos do que falam, ou seja, nada!

CAPÍTULO VIII – METÓDOS DE SEGURANÇA DE DADOS

Criptografia

A criptografia, tão antiga como a própria escrita, é um dos métodos mais eficientes de se transferir informações, sem que ninguém não autorizado consiga obter essa informação.

Uma informação baseada em chaves, pode ser codificada através de um algoritmo de criptografia, o que chamamos de encriptação e tendo-se o conhecimento do algoritmo e da chave utilizada é possível recuperar a informação original, o que chamamos de decriptação.

Na criptografia moderna, possuímos características que a fazem su*bbanco de dados*ividir-se em dois grandes grupos:

- Criptografia de Chave Simétrica;
- Criptografia de Chave assimétrica.

Criptografia de Chave Simétrica:

A Criptografia de Chave Simétrica é a criptografia tradicional, onde a mesma chave utilizada na codificação deve ser usada na decodificação. Dentre outros, podemos citar alguns algoritmos de Chave Simétrica: *IDEA (International Data Encryption Algorithm*), DES (*Data Encryption Standart*) da IBM e o RC2/4, da RSA Data Security.

A Criptografia Simétrica é muito eficiente em conexões seguras na *Internet*, onde os processos computacionais trocam senhas temporárias para algumas transmissões. Um exemplo bem comum é quando navegamos pela *Internet* nos *sites* onde geralmente são preenchidos dados sigilosos, e é mostrado a seguinte mensagem:

- "Você está utilizando o SSL (*Secure Sockets Layer*)", que funciona à base de criptografia simétrica, muito provavelmente um DES ou algo da RSA.

Criptrografia de Chave Assimétrica:

Estudos realizados há uns 20 anos tornaram possíveis algorítimos de criptografia utilizando duas chaves. Criptorafando com a chave A, só seria possível a decriptação com a chave B.

Chave Pública e Chave Privada

Essa assimetria gera uma nova abordagem, a de chave pública e privada. Tendo duas chaves não precisamos ficar presos a essa troca para o processo de codificação/decodificação, já que cada um deverá possuir sua chave pública e sua chave privada.

Uma chave privada é de conhecimento única e exclusivamente de quem irá enviar a mensagem, já a pública deve estar disponível a quem quiser lhe enviar informações encriptadas.

Como a encriptação/decriptação depende das duas chaves, ao enviar uma mensagem deve-se encripta-la com a chave pública do destinatário, assim quando esta chegar ao destino será decriptada com a chave privada, que é de conhecimento exclusivo do mesmo. Então, mesmo se a mensagem for interceptada por terceiros não poderá ser lida.

Assinatura Digital

A assinatura digital é um dos maiores avanços em relação à autenticidade da informação. Como a criptografia por chaves simétricas vale para ambos os lados Pública >> Privada e Privada >> Pública, podemos assegurar a nossa identidade como autores de determinada mensagem.

Exemplo: Se encriptar-mos uma mensagem com nossa chave privada, a única chave capaz de decriptá-la é a chave pública, com isso todas as pessoas que possuírem esta chave pública poderão ler a mensagem e isso não é vantajoso, por outro lado, como as

únicas pessoas que sabem da nossa chave primária somos nós mesmos, está assegurada nossa identidade como autores dessa mensagem.

Criptografia + Assinatura Digital

A utilização de ciptografia e assinatura digital se dá com o uso de quatro chaves.

O primeiro passo é criptografar a mensagem com nossa chave privada, depois criptografar novamente a mensagem com a chave pública do destinatário. Quando essa mensagem chegar ao destino o processo de decriptação deverá ser feito da seguinte forma: Primeiro a mensagem deverá ser decriptada com a chave privada do destinatário, e depois decriptada novamente com a chave pública do remetente

Chaves Simétrica e Assimétrica

A Criptografia com a chave assimétrica tem uma desvantagem considerável para os tempos modernos, ela é muito lenta, e dependendo do computador um texto pode levar de minutos à algumas horas, o que torna-o extremamente viável, por outro lado, a simétrica é rápida mas possui o problema da chave única que a torna insegura.

Levando em consideração esses fatos, a solução imediata seria a seguinte: Primeiro a de criptografar a mensagem com a chave simétrica (isso tornará a mensagem rápida, porém não segura); em seguida criptografar novamente a mensagem com a chave pública do destinatário (isso tornará a mensagem segura, já que somente o destinatário poderá decripta-la com sua chave privada).

Apesar de parecer a forma mais confiável, quando criptografamos uma mensagem de forma simétrica-assimétrica, esbarramos em mais um problema: Perde-se a autenticidade da mensagem, pois dessa forma não temos como comprovar quem enviou a mensagem.

Message Digest:

O Message Digest é uma maneira de criar-se um código à partir de uma mensagem à ser enviada. Esse código é um cojunto de caracteres que reflete o conteúdo da mensagem. Os algoritmos mais utilizados no mercado para gerar o Message Digest são: MD4/5 e o SHA (*Secure Hash Algorithm*).

O Message Digest possui duas características fundamentais:

- Não é possível inverter o cálculo sobre o Message Digest para recuperar a mensagem original;
- Message Digest é único por mensagem, ou seja, não pode existir o mesmo Message Digest para mensagens diferentes.

Com essa ferramenta fica assegurada a autenticidade utilizando a criptografia assimétrica. Porém se quisesse-mos enviar uma mensagem "não confidencial", primeiro iríamos calcular o Message Digest da mensagem, depois encriptar esse Message Digest com nossa chave privada, e a seguir enviar a mensagem e o Message Digest encriptado. Quando o destinatário receber a mensagem, ele irá calcular o Message Digest da mensagem e comparar com o Message Digest enviado (utilizando a chave pública para decriptá-lo). Se o Message Digest enviado for igual ao calculado pelo destinatário, ele terá certeza de quem o enviou.

Mas a mensagem em si foi enviada sem criptografia, e qualquer pessoa poderia ter lido. Com isso a mensagem passa a ter autenticidade, mas perde a segurança.

Então a solução mais segura, autêntica e adequada seria a seguite:

Vamos supor que quisesse-mos enviar uma mensagem grande, criptografada e assinada (ou seja, segura e autentica) no menor tempo possível.

Primeiro criamos um Message Digest da mensagem e o encriptamos com a nossa chave privada (isso torna a mensagem autêntica), depois encriptamos a mensagem inteira

com uma chave simétrica (isso torna a mensagem rápida), e então encriptamos a chave simétrica com a chave pública do destinatário (isso torna a mensagem segura).

Então envia-se tudo: o Message Digest encriptado com nossa chave privada, a mensagem criptografada com a chave simétrica, e a chave simétrica encriptada com sua chave pública.

Ao receber a mensagem o destinatário deverá primeiro decriptar a chave simétrica com sua chave privada, depois com a chave simétrica decriptada, decriptar a mensagem. Em seguida, decriptar o Message Digest com a nossa chave pública e depois calcular o Message Digest da mensagem original.

Feito isso é só comparar os dois Message Digest: o que foi enviado, e o que foi calculado, se forem iguais o destinatário terá a certeza de que fomos nós que enviamos a mensagem e a mensagem não sofreu nenhuma alteração.

GLOSSÁRIO

CONCLUSÃO

BIBLIOGRAFIA

BENNETT, Geoff. *Internet*working com TCP/IP. – Rio de Janeiro: Editora IBPI.

BORLAND, Russell. Introdução ao Windows 98. Tradução: Vanderberg Dantas de Souza. – Rio de Janeiro: Editora Campus, 1998.

CRUMLISH, Christian. Dicionário da *Internet*. – Rio de Janeiro: Editora Campus.

FRAZIER,Deneen & KURSCHAN, Barbara & ARMSTRONG, Sara. *Internet* Para Estudantes. – Rio de Janeiro: Editora IBPI.

GOMES, Olavo José Anchieschi. Segurança Total. – São Paulo: Editora Makron Books, 2000.

HONEYCUTT, Jerry. Introdução ao Microsoft Windows 2000 Professional. Tradução: Edson Furmankilwicz. – Rio de Janeiro: Editora campus, 1999.

MACHADO, Francis B. & MAIA, Luiz Paulo. Arquitetura de Sistemas Operacionais – 2ª edição. – Rio de Janeiro: Editora LTC, 1999.

SALOMON, David A. Desvendando o Windows NT. Tradução: [da 2ª edição original]: Daniel Vieira. – Rio de Janeiro: Editora Campus, 1998.

SILBERSCHATZ, Abraham; KORT, Henry F. & SUDARSHAN, S. Sistemas de B*anco de dados*. – São Paulo: Editora Makron Books, 1999.

SOARES, Luiz fernando G.; LEMOS, Gruido & COLCHER, Sérgio. Redes de Computadores: das LANs, MANs e WANs às redes ATM – 6ª edição. – Rio de Janeiro: editora Campus, 1995.

SPYMAN. Manual Completo do Hacker – 3ª edição espacial. – Rio de Janeiro: Editora Book Express, 2000.

TANENBAUM, Andrew S. Redes de Computadores – 5ª edição. Tradução [da 3ª edição original]: Insight Serviços de Informática. – Rio de Janeiro: Editora Campus, 1997.

_____. Sistemas Operacionais Modernos. Tradução: Nery Machado Filho. – Rio de Janeiro: Editora LTC, 1992.

www.anti-hackers.com.br

www.clubedohardware.com.br

www.compaq.com.br