POLÍTICA DE SEGURANÇA COMPUTACIONAL

Prof. Dr. Tito Lívio Gomes Osório

Tenho a perfeita consciência que destruir é sempre mais fácil, mais simples e mais rápido do que construir.

Dedico esta obra a todos aqueles que passam grande parte do seu tempo no estudo da ciência e da tecnologia e, em especial, àqueles que lutam diariamente para preservar a integridade e a segurança das instituições.

Tito Lívio

MP, maio 2004

RESUMO

Na era da INTERNET, nenhuma empresa pode abrir mão de se comunicar eletronicamente com os sues cliente e fornecedores, todavia, se o uso dessa tecnologia permite a redução dos custos e garantam agilidade dos serviços, ao mesmo tempo representam riscos consideráveis para com a sua integridade e inviolabilidade.

Apesar de não tomarmos conhecimento de forma direta, diariamente empresas dos mais variados ramos de atividades sofrem ataques de "hackers" o que lhes ocasionam perdas de considerável valor. Alia-se a isso a proliferação de "vírus computacionais" que em sua passagem destruidora, provocam perdas, a mais das vezes irrecuperáveis.

Diante deste quadro estaremos ao longo dessa publicação abordando os aspectos fundamentais para se implementar e avaliar as Políticas de Segurança Computacionais nos seus aspectos básicos.

Assim sendo, iremos abordar os seguintes tópicos gerais:

- Segurança de Dados;
- Segurança dos Sistemas Gerenciadores de Bancos de Dados;
- Segurança dos Sistemas Operacionais;
- Segurança dos Sistemas de Informação;
- Segurança das Comunicações de Dados;
- Assinatura Digital;
- Vírus de Computadores; e
- Criptografia e Assinatura Digital.

Finalmente faremos uma explanação sobre os principais tipos de ataques, e como preparar defesas a esses ataques de forma a garantirmos eficiência e segurança em nossas atividades.

ÍNDICE

I N T R O D U Ç Ã O

A Tecnologia da Informação vem, desde o início e durante toda essa sua existência, forçando o desenvolvimento da tecnologia e de seus recursos. O objetivo inicial de diminuir o trabalho repetitivo e manual e, ainda, possibilitar a realização de atividades com melhor qualidade encara desafios diários, frutos da globalização da economia, da abertura de mercado e da livre concorrência, na busca constante do domínio do Estado da Arte.

A avanço da tecnologia disponível é tanto que atualmente não necessitamos sair de nossas casas para realizarmos operações as mais variadas possíveis. Atualmente, operações tais como: compra de mercadorias em geral, transações bancárias e outras atividades corriqueiras do nosso dia-a-dia e, até mesmos cursos os mais variados possíveis, estão ao nosso alcance com apenas um "clique" nos nossos computadores, ou seja "On Line".

O crescimento e a disponibilização das facilidades da tecnologia fez com que a Tecnologia da Informação deixasse de ser objeto de uso somente de especialistas, passando para o domínio dos usuários em geral, mesmo para aqueles que sem muito conhecimento técnico, que, com algum esforço, aprenderá o básico para a sua sobrevivência na "selva" da informação. Indubitavelmente, o avanço da tecnologia trouxe muitas inovações e, dentre elas, surgiu uma de real importância – a Rede Mundial de Computadores – INTERNET, ferramenta poderosa e moderna de distribuição das informações e que trouxe benefícios de considerável monta para aqueles que souberam e sabem aproveitar do presente Estado da Arte.

Todavia, a necessidade da abertura do mercado, a competitividade e o empreendedorismo trouxeram em sua avalanche avassaladora novas discussões, e obrigou a todos os técnicos a travarem uma batalha dioturna entre o "bem e o mal". De um lado profissionais criando e abrindo o mercado com produtos os mais variados, facilitando a vida de todos e, do outro, agentes da destruição, agindo solitariamente ou em grupos, buscando destruir, desordenar o mercado, auferir lucros em atividades ilícitas, lesar, criar instabilidades, gerar a insegurança a níveis jamais vistos (quem não se lembra das tristes imagens do fatídico 11 de setembro de 2001).

Nos últimos anos vêm acontecendo violações as mais variadas possíveis, onde grupos de "hackers" invadem computadores de "sites" dos mais simples aos mais complexos e imputam perdas significantes em valores monetários diretos, ou simplesmente destroem anos e anos de trabalho, pelo simples fato de se sentirem "poderosos". Tais fatos vêm obrigando as empresas a se preocuparem mais e mais com os aspectos da segurança computacional.

Assim sendo, o tema "SEGURANÇA COMPUTACIONAL" passou a fazer parte do nosso cotidiano e nos impele a buscar o aprimoramento dos nossos conhecimentos para que não sejamos surpreendidos com fatos desagradáveis e irremediavelmente destruidores.

Uma série de perguntas paira sobre as nossas cabeças:

- Nossos Sistemas de Informação são seguros?
- Há uma conscientização dos nossos usuários para com os aspectos gerias de segurança?
- Nosso Banco de Dados é seguro e mantém a sua inviolabilidade e preserva os dados?
- Nossa intranet e extranet são protegidas contra violações e interceptações de mensagens?
- Estamos absolutamente protegidos, ou nos faltam conhecimentos que nos permita operacionalizar níveis de segurança que possibilitem oferecermos serviços de qualidade, com a abertura requerida, e com segurança?

Ao respondermos essas questões estaremos traçando os destinos das nossas empresas – seguras ou violáveis.

A Política de Segurança Computacional refere-se a um conjunto de leis, de regras e de práticas que normalizam como uma organização gerencia, protege e distribui as suas informações e recursos computacionais.

Ainda que ataques de *hackers e crackers* sejam muito comentados e estejam em evidência, eles não são tão numerosos quanto os problemas internos de segurança que ocorrem nas empresas. A implementação de uma Política de Segurança Computacional baseia-se na aplicação de regras que limitam o acesso de uma entidade aos dados, às informações e/ou aos recursos computacionais disponíveis, com base na comparação dos níveis funcionais e da necessidade de autorizações de acesso às informações. Assim sendo, essa Política deverá definir o que é e o que não é permitido durante a operação dos Sistemas de Informação, evitando e/ou prevendo a possibilidade da ocorrência de ataques, de modo a proteger os dados e as informações.

O documento que contém a Política de Segurança Computacional deve:

- Trazer explicações da importância da adoção dos procedimentos de segurança, justificando-os junto aos usuários, para que o entendimento dos mesmos leves aos referidos usuários ao comprometimento pessoal com todas as ações de segurança adotadas;
- Relacionar os recursos que se protege e quais os que estão disponíveis, relatando quais os níveis em que estão liberados e em quais atividades;
- Relatar o que acontece quando softwares, dados e ferramentas não homologadas são detectados no ambiente computacional;

O perfeito funcionamento de uma Política de Segurança depende muito do conhecimento do seu conteúdo e da cooperação dos usuários nos seus diversos níveis. Ele deve ser incentivado a sentir que as medidas de segurança foram adotadas visando o seu próprio benefício.

Segundo ANDREWS THOME HORKERS – Manager Security da Internet Security Systems:

> **"O principal problema para implementar uma Política de Segurança é a cultura das pessoas, pois é preciso reeducar os funcionários e mostrar para eles que os ativos e os equipamentos das empresas devem ser protegidos, que as senhas não devem ser divulgadas e que as informações confidenciais não devem estar disponíveis" (ISS - Oct 2002).**

CAPÍTULO I

SEGURANÇA DE DADOS

CAPÍTULO I
SEGURANÇA DE DADOS

Um dos maiores problemas e certamente um dos mais difíceis de ser resolvido é o da segurança dos dados. O problema tem muitas facetas e envolve diversos fatores tais como: instalações físicas; procedimentos operacionais; características de "hardware"; especificações de "software" e outras mais que iremos discutindo ao longo deste capítulo.

Vivemos uma sociedade moderna na qual a informação é de fundamental importância, quer no dia-a-dia das pessoas ou nas rotinas de trabalho das empresas, daí a necessidade de mantermos mecanismos de segurança capaz de garantir a integridade e inviolabilidade dos dados.

A segurança dos dados pode ser definida como a proteção dos mesmos contra revelações de seus conteúdos, quer acidentalmente, quer intencionalmente a pessoas não autorizadas, contra violações e possíveis alterações de conteúdo sem que para isso esteja autorizado. Seu universo se divide em duas visões:

- **Segurança Física –** Neste aspecto devemos atentar para ameaças sempre presentes e que às vezes passam desapercebido tais como: incêndios, desabamentos, inundações e alagamentos, problemas com as redes elétricas, acesso indevido ao CPD, treinamento inadequado, etc.

Assim, medidas de proteção físicas tais como: serviços de guarda, uso de sistemas "no-breaks", utilização de alarmes, circuitos internos de televisão, monitoramento e controle de acesso às áreas de caráter privativo e outras medidas de segurança devem ser adotadas.

- **Segurança Lógica –** Este aspecto é muito mais abrangente e complexo, requerendo, conseqüentemente, um estudo muito mais apurado e detalhado. Devemos estar atentos aos mínimos detalhes que compõem este tipo de segurança. Assim sendo, no decorrer deste trabalho iremos dar atenção especial para este tipo de segurança.

A Tecnologia da Informação, no seu nível abstracional mais elevado, prevê a atuação em um ambiente computacional indivisível conforme a figura abaixo:

Ambiente computacional

1.1 – DADOS E INFORMAÇÕES

Diariamente nos referimos aos dados e deles fazemos uso de forma contínua, todavia ao tentarmos definir corretamente o que significam, normalmente cometemos erros e o definimos como uma parte da informação etc. Todavia, observando a figura acima e comparando com a definição adotada pela Universidade de Harvard, podemos concluir a exatidão desta definição:

"Dado é a unidade básica do conhecimento humano"

Conseqüentemente podemos chegar à definição de Informação:

"Informações são conhecimentos adquiridos a partir do processamento de um conjunto de dados"

A indivisibilidade do ambiente computacional vista acima, nos leva a afirmar que todas as ações pelas quais passarem os dados, refletirão de maneira direta nas informações por eles geradas. Assim, salvaguardar a integridade e a inviolabilidade dos dados terá reflexos diretos na qualidade das informações produzidas.

Resta-nos questionar para que servem as informações? E, novamente, nos encontraríamos em situação de extrema ambigüidade e para a qual nem sempre encontramos a resposta adequada. Porém, se analisarmos o mundo em que vivemos, poderemos facilmente deduzir que: **"A informação é a principal ferramenta do processo decisório".** No mundo moderno ninguém mais pode decidir de forma abstrata ou mesmo por pura intuição. Não podemos arriscar e levar nossas empresas ao fracasso, pelo simples fato de não possuirmos as informações necessárias em tempo hábil.

Com relação aos dados, as empresas devem aplicar os seguintes preceitos:

- **Dados Modelados –** Os dados devem ser identificados na sua composição e semântica, estudados no seu formato, origem, natureza e seu relacionamento com outros dados, ou classe de dados.

- **Dados Resguardados** – Os dados deverão atender aos requisitos básicos de segurança e de integridade.

- **Dados Disponibilizados** – Deverão ser disponibilizados um conjunto de ferramentas que permitam o acesso aos dados e que promovam a sua atualização, de forma a gerar informações atualizadas para a tomada de decisão.

Desta forma, há que se observar alguns requisitos fundamentais para a perfeita obtenção desses preceitos.

1.2 - REQUISITOS FUNDAMENTAIS DOS DADOS

Para gerarmos informações precisas devemos fazer com que os dados tenham **todos** os requisitos abaixo relacionados definidos como fundamentais para os mesmos.

- **Credibilidade -** O dado deve ser real e representar a verdade.

- **Confiabilidade –** O dado deve ter uma origem confiável, ou seja, o dado deve ser captado na sua principal e única origem.

- **Consistência –** Um mesmo dado não pode assumir dois valores diferentes no mesmo intervalo de tempo.

- **Oportunidade –** Todo o dado tem um tempo de vida útil para o qual poderá informações oportunas.(1)

➢ **Portabilidade –** O dado deve poder ser levado a outro processamento, sem que perca a sua forma e conteúdo. Caso o dado seja processado de forma igual, porém em tempos diferentes devem gerar informações iguais.

➢ **Corporatividade –** O dado deve ser corporativo, ou seja, deve pertencer a empresa como um todo e não a algumas atividades. O mesmo dado deve atender a diversas atividades.

➢ **Interoperabilidade –** O dado deve ter a capacidade de ser operado e processado por diversas atividades da empresa sem que perca seu valor inicial.

➢ **Segurança –** O dado deve ser preservado em sua inviolabilidade e resguardado de acessos não permitidos.

> (1) - Este conceito deverá ser submetido a uma reformulação conceitual, ou ser abandonado, pois em uma visão mais moderna surgem as "**Datawarehouses"** que utilizam dados bastante antigos para utilização em Sistemas de Informações Estratégicas (EIS) que se utilizam séries históricas na formação destas informações.

O processamento eletrônico de dados é formado por um conjunto de operações pelas quais os dados são submetidos e para as quais devemos ter uma observação constante.

1.3 – OPERAÇÕES COM DADOS

Antes de definirmos as operações possíveis com dados, devemos caracterizar algumas ações que, quando executadas podem ou não alterar os valores iniciais deles. Existem duas classes de ações:

➢ **Ações Não Degenerativas –** grupo de ações que, quando realizadas, não alteram o valor inicial do dado.

➢ **Ações Degenerativas –** grupo de ações que, quando realizadas, alteram o valor inicial do dado.

O processamento eletrônico de dados é constituído de duas operações perfeitamente distintas:

➢ **Operações de Manipulação de Dados –** neste grupo estão incluídas as seguintes operações:

- Consultar Dados
- Incluir Dados
- Alterar Dados
- Excluir Dados

➢ **Operações de Processamento de Dados –** neste grupo estão incluídas as seguintes operações:

- Lógicas
- Aritméticas

De posse dos conceitos acima podemos, então, agregar conhecimentos e definirmos as operações e ações com os dados, se não vejamos: se realizarmos **operações de manipulação de dados**, tais como: **alterar, incluir e excluir** estaremos alterando os valores iniciais dos mesmos, o que nos leva a afirmar que essas operações acarretam em **ações degenerativas**, todavia ao realizarmos **operações de processamento de dados**, não importando qual delas é executada, e **operações de manipulação de dados** (consulta de dados) estaremos realizando **ações não degenerativas.**

Agregar este conhecimento, apesar de parecer um pouco simplório, é de fundamental importância para a obtenção e a preservação dos requisitos fundamentais anteriormente definidos. Todavia, a sua total compreensão somente poderá ser obtida quando agregarmos um novo conhecimento, baseado nos tipos fundamentais de usuários de dados.

1.4 – TIPOS DE USUÁRIOS DOS DADOS

Existem basicamente dois tipos de usuários em processamento eletrônico de dados, ambos com características perfeitamente definidas, resta-nos somente definir quais as operações que estarão disponíveis para cada um deles, e compreender perfeitamente bem como uma Política de Segurança de Dados alcançará o sucesso desejado, a partir da adoção de medidas restritivas de acessibilidade aos dados. Assim podemos definir os seguintes tipos de usuários:

1.4.1 - <u>Usuários Operacionais ou de Processamento</u> - são definidos como aqueles que necessitam utilizar os dados para qualquer tipo de processamento gerando informações. Como já vimos anteriormente, as operações de processamento são baseadas em ações não degenerativas, logicamente restringindo a acessibilidade a essas operações, não correremos o risco de alterações dos valores iniciais dos dados. Resta-nos somente definir o nível de acesso de cada um desses usuários (de acordo com as restrições de acessos) para termos a certeza de que parte da nossa intenção de preservar os dados estará sendo alcançada.

1.4.2 - <u>Usuários Fonte</u> - Chamamos de usuários fonte àqueles usuários que dão origem inicial ao dado, aquele que gera o dado. Esses usuários devem ser criteriosamente escolhidos, pois são de fundamental importância para a empresa. A eles e somente a eles devem ser fornecidas acessibilidades para que realizem operações de manipulação de dados que se baseiam em ações degenerativas. Logicamente esses usuários são os principais responsáveis pela garantia dos principais **requisitos fundamentais dos dados,** se não vejamos:

- Se o dado não representar a verdade (incrédulo), ele não o incluiu/alterou corretamente;
- Se o dado não for confiável este usuário não é confiável e deve ser substituído;
- Se o dado não tiver consistência houve erro na criação deles, ou existem duplicações de dados;
- Se o dado não é atualizado, está havendo erro na sua atualização, ou sobrecarga de trabalho;

Conforme pode ser observado, fica bastante fácil determinar-se responsabilidades com os dados e exigir-se segurança a partira do uso desses critérios e identificarmos os responsáveis pela má utilização e/ou manipulação dos dados.

Um **Usuário Fonte** pode vir a ser também um **Usuário Operacional**, todavia para estes casos devem ser bem separadas e analisadas essas duplicidades funcionais para que não firam os conceitos acima determinados.

1.5 – RESTRIÇÕES DE ACESSO AOS DADOS

Além das ações acima relatadas, a garantia da integridade dos dados prevê, ainda, outras ações que permitirão a criação de rotinas gerais de administração dos mesmos. Assim a cada acesso a um dado ou grupo de dados devemos seguir os seguintes passos:

- **Identificar o Usuário -** o usuário deve ser identificado, para tal ele deve possuir uma senha e uma identificação de acesso("login") que determina a sua acessibilidades e qual o seu nível de acesso dos dados;

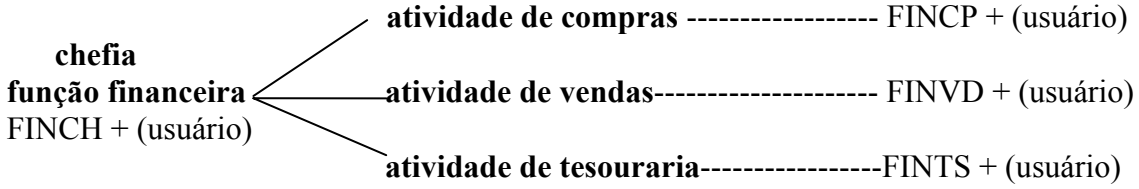
- **Validar o Usuário -** a partir da validação da sua senha e do seu "login", o usuário deve ser transportado para a sua área de acesso, onde passará a ter os dados disponibilizados com total controle;

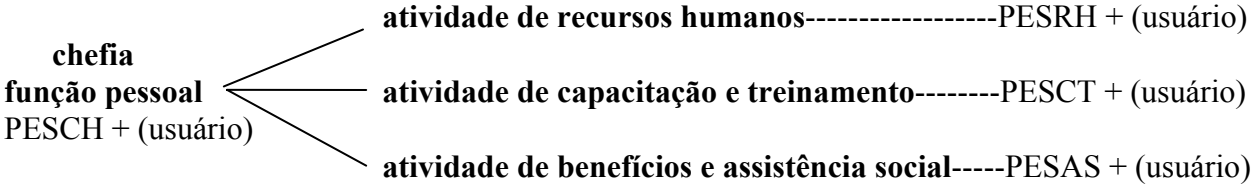
- **Conceder Privilégios** - Aos usuários, dependendo do nível em que se encontram poderão ser concedidos privilégios, desde que não venham a ferir os níveis de acessibilidades e segurança. A concessão de privilégios é de responsabilidade da Gerência Geral de Processamento, em conformidade com as necessidades apresentadas pelo Administrador de Bancos de Dados(DBA). Em empresas que possuem um Manager Systems Security (MSS) este deve participar da avaliação de concessão dos privilégios.

A concessão de privilégios e acessibilidades pode levar em consideração aspectos funcionais dentro da empresa, assim os privilégios passarão a gerar **senhas por grupos funcionais** que identificarão as funções departamentais de cada um dos usuários, além da identificação pessoal do mesmo. A garantia do nível de acessibilidades também estará sendo obtida, pois esta senha grupal deverá adotar o que chamamos de **senhas por herança hierárquica** em diversos níveis.

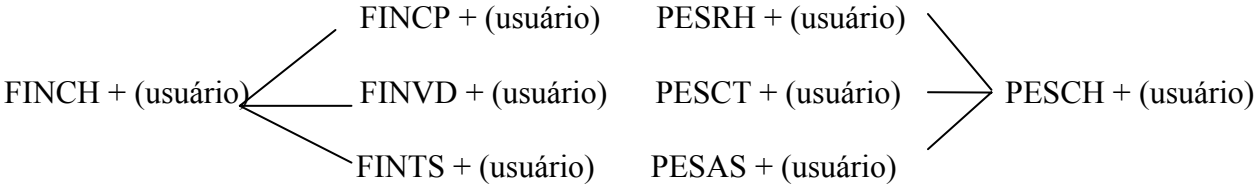
Essas **senhas por herança** podem ainda conter o que denominamos de **heranças múltiplas funcionais,** ou seja, um mesmo usuário tem acessibilidades a grupos de dados cuja origem têm outras funções diferentes da sua.

Vejamos como funcionam as senhas grupais com a determinação de heranças simples e múltiplas. Imaginemos que uma empresa tenha duas Funções (Departamentos) diferentes, aos quais estarão subordinadas algumas atividades, conforme descrito abaixo:





Assim a senha por herança simples e/ou múltiplas poderiam ser vistas assim:



A concessão de senhas funcionais e as senhas por herança são extremamente eficientes, todavia devem ser criteriosamente estudadas, pois, ao cancelarmos os privilégios dos níveis de cima, estaremos cancelando os privilégios por herança dos níveis imediatamente abaixo.

Nada que não se possa contornar, somente requer um pouco mais de atenção, porém há que se ressaltar que esta prática, apesar de trabalhosa inicialmente, produz significativos resultados práticos na preservação da segurança de dados e de Sistemas de Informação, sendo assim adotada por empresas de médio e de grande porte, que atingiram níveis de segurança elevados.

- **Manter Arquivos de "log"** - O sistema deverá prever que a cada "login" o usuário tenha a sua identificação, hora de acesso e, dependendo do sistema, o que ele realizou com os dados, devidamente registrados no que chamamos de Arquivos de Log. Esses arquivos deverão ser periodicamente avaliados pelo DBA e/ou MSS e, em caso de má utilização e/ou violação, tomar as medidas necessárias a evitar que tais fatos se repitam, ou mesmo chamando a atenção dos usuários que negligenciarem na operação com os referidos dados.

1.6 - BACKUP

O "backup" é uma cópia dos arquivos que julgamos ser, talvez, a mais importante ação no sentido da preservação dos arquivos chaves (fundamentais) de uma empresa. Com o uso cada vez mais acentuado dos computadores, um sistema de "backup" que garanta a segurança e a disponibilidade "full-time" dos dados corporativos da empresa é fundamental. Apesar de ser uma medida de segurança antiga muita empresas não possuem uma política adequada de "backups", ou mesmo não o fazem de forma correta.

Montar um sistema de "backup" requer um pouco de cautela. É importante, por exemplo, saber escolher o tipo de mídia para armazenamento dos dados, tais como: fitas magnéticas, discos óticos, ou sistemas RAID. No Brasil, tal como em outros países, o dispositivo mais usado é o "Digital Áudio Tape", pois oferece uma capacidade de armazenamento de até 16 Gby, a um custo bastante razoável, cerca de um centavo de real por megabyte.

Pequenas empresas, não requerem grandes investimentos para a implantação de um sistema de "backup", sendo os mais utilizados os que trabalham com drivers externos do tipo "ZIP e JAZ", equipamentos de baixo custo operacional e de manutenção e que possuem capacidade de armazenamento capaz de atender as necessidades dessas empresas.

Embora as mídias óticas se mostrem como a última palavra em armazenamento, para o uso específico em "backup" elas não são viáveis, pois possuem uma capacidade de armazenamento relativamente pequena, cerca de 600 Mby em cada Compact Disk, além não serem regraváveis com facilidade. Todavia um ponto bastante vantajoso para as mídias óticas é a segurança com que podem ser armazenados os dados. Há que se observar que as mídias magnéticas vêm sendo hoje em dia para a

criação de **bibliotecas de dados,** o que caracteriza uma forma de armazenamento de dados e não um sistema de "backup".

A tecnologia RAID consiste em um conjunto de drivers que são vistos pelo sistema operacional como uma única unidade de disco, continuando a propiciar o acesso aos dados, mesmo que um dos discos venha a falhar. Os dados passam pelo nível 1 que significa um espelhamento do driver, ou servidor (cópia dos dados do driver, ou do servidor), até o nível 5 que é o particionamento com paridade (o mesmo arquivo repetido em diferentes discos). Esta tecnologia é, sem dúvidas, uma opção segura e confiável, e vem sendo muito utilizada em empresas que possuem redes do tipo "non stop" e que não podem perder tempo interrompendo o sistema para fazer o "backup".

Após a escolha da mídia adequada ao armazenamento, é muito importante decidir qual o "software" será utilizado para a realização do "backup". São três os requisitos básicos que devem ser observados:

- Facilidade de automatização;
- Facilidade de recuperação; e
- Facilidade de Gerenciamento.

Isso significa que a ferramenta deve realizar, sem a intervenção humana, um conjunto de rotinas, tais como: abrir a base de dados, copiar somente os arquivos que foram alterados e fechar a base de dados. É importante que o produto possa realizar o gerenciamento centralizado, permitindo fazer o "backup" tanto dos arquivos individualmente, quanto do banco de dados geral através de uma mesma interface.

Assim resta-nos sugerir algumas regras para que possamos fazer a escolha correta de um sistema de "backup":

- Procure o tipo de mídia de armazenamento adequada ao volume de dados e às necessidades de sua empresa;

- O ramo de atividades de sua empresa também é muito importante. Companhia que utilizam sistemas "non stop" necessitam de sistemas de "backup" rápidos e seguros;

- Os "softwares de backup" devem realizar tarefas de forma automáticas, tais como: cópias periódicas dos dados, atualização dos arquivos que foram modificados, etc;

- Se a empresa possuir um grande banco de dados, é importante que a ferramenta gerencie através de uma mesma interface tanto o "backup" dos arquivos quanto do próprio banco de dados;

- É muito mais fácil e seguro o gerenciamento do "backup" de toda a rede de forma centralizada, mesmo em se tratando de redes abertas e heterogêneas.

Finalmente, um mercado novo vem surgindo e com ele uma prática que vem sendo adotada para empresas que utilizam a INTERNET é o de sistemas de "Web backup". Neste sistema as empresas alugam um espaço no servidor "web" para armazenamento do "backup" dos seus dados, podendo atualizá-los e/ou carrega-los quando houver necessidade. *Nesta prática a prestadora do serviço passa a ser a responsável pela segurança do "backup"?.*

Todavia, esta prática não oferece, ainda, uma solução adequada para o "backup" das empresas, pois, existem dois problemas básicos a serem definidos: a falta de infraestrutura e a falta de mecanismos de segurança que possam preservar a integridade dos dados armazenados nos prestadores

de serviços "web". Nenhuma empresa deseja ter os seus dados armazenados em um lugar qualquer (indefinido) na INTERNET.

Outro ponto importante e que sempre é bom lembrar, é que a grande maioria das falhas na rede corporativa é fruto de erros humanos, o que significa que seria necessário um treinamento adequado dos envolvidos neste tipo de operação, para que os sistemas de "web backup" pudessem contar com a ação imediata e correta dos envolvidos, em casos de emergências e falhas dos sistemas principais.

Outra falha bastante comum encontrada nas empresas, além do despreparo dos profissionais envolvidos, é o armazenamento em discos, ou outra mídia qualquer, permanecendo a cópia de segurança no mesmo local físico dos dados originais. Em caso de desastres e/ou situações de calamidades, tais como incêndios, enchentes, etc, ocorrerá uma perda total dos dados.

Concluindo devemos adotar um plano de segurança das cópias de "backup" que vão desde a política de obtenção das referidas cópias até a um plano de contingência para o caso da ocorrência de situações de calamidades. Todavia, o treinamento do pessoal envolvido nesta atividade é fundamental.

C O N C L U S Ã O

Conforme podemos depreender das medidas propostas relatadas acima, os objetivos fundamentais da **Segurança dos Dados** envolvem aspectos muito abrangentes. Seu estudo e a adoção de medidas preventivas e corretivas visam desde a proteção dos dados contra a ação criminosa dos "hackers", até a má operação em processamento e/ou manipulação dos dados, de forma intencional ou inadvertidamente. Sobre tudo a **Segurança dos Dados** visa preservar a integridade do principal patrimônio que possui a empresa - os seus dados.

Podemos ainda, classificar as ações que buscam a violação dos dados de acordo com os seguintes tipos de infiltrações:

- **Infiltração Deliberada -** esta infiltração tem como objetivo principal conseguir o acesso aos dados e/ou às informações de forma deliberada, com ataques frontais ou laterais (que estaremos definindo oportunamente) para descobrir informações de seu interesse, aferindo lucros pessoais ou para grupos de concorrentes, exemplo típico da atuação de "crackeres"; para alterar ou destruir arquivos; e para obter livre acesso aos recursos dos sistemas computacionais, sem que para isso esteja autorizado.

- **Infiltração Ativa -** esta infiltração consiste desde o exame periódico dos conteúdos das cestas de lixo das áreas de processamento, até a gravação (cópia) clandestina dos dados da empresa. Segundo alguns especialistas essas infiltrações incluem os seguintes tipos de ações:

  - *SAPEAR* - que consiste no uso de um acesso legítimo ao sistema para obtenção de informações para as quais não está autorizado;

  - *USAR DISFARCE* - consiste na prática de utilizar a identificação pessoal para efetuar gravações troca clandestinas de níveis de acesso e, posteriormente, acessar o sistema como legítimo usuário;

  - *Identificar e usar Alçapões* - consiste na utilização das características do "hardware", limitações e imperfeições do "software" e/ou pontos de entrada (portas) especialmente implantadas que permitirão que pessoas não autorizadas tenham acesso aos sistemas;

  - *Uso de Canais* - esta prática consiste em utilizar a fragilidade dos canais ativos de comunicações para invadir os sistemas. Esta pratica é bastante utilizada por "hackers" e "crackers", sendo a sua principal forma de atuação.

  - *Uso de meios Físicos* - esta prática consiste em violar os sistemas a partir de uma posição na área de processamento, por profissionais da própria empresa com acesso aos dados, buscando de forma deliberada passarem informações a terceiros.

Assim sendo, as Políticas de Segurança Computacional devem prever aspectos de Segurança de Dados, pois estes são na realidade a parte mais crítica da Tecnologia da Informação e devem conter ainda um **Plano de Contingência,** para o caso de ocorrerem problemas de violação.

Todavia, é oportuno frisar que ***SEGURANÇA ABSOLUTA E TOTAL*** não existe e que empresa nenhuma estará imune a qualquer uma dos fatores físicos e/ou lógicos que podem colaborar para violações e perdas dos dados, temos é que elaborar uma política de segurança abrangente e que nos permita uma ter uma segurança homogênea e suficientemente clara, que atinja todos os níveis da

empresa e que sobre tudo passe por avaliações constantes para que se modernize a cada momento, tal qual a tecnologia. Nossos adversários estudam cada vez mais e descobrem formas cada vez mais eficientes de violar e prejudicar o nosso trabalho.

Devemos sempre perguntar:

- **Proteger O QUE?**
- **Proteger DE QUEM?**
- **Proteger A QUE CUSTO?**
- **Proteger COM QUE RISCO?**

O principal axioma da segurança é por demais conhecido de todos, mas nunca é demais recordar:

"UMA CORRENTE NÃO É MAIS FORTE DO QUE O SEU ELO MAIS FRACO"

CAPÍTULO II

SEGURANÇA EM BANCOS DE DADOS

CAPÍTULO II
SEGURANÇA EM BANCOS DE DADOS

A segurança das informações, como um todo, depende do esquema de segurança do Banco de Dados (BD) onde as mesmas estão armazenadas. Quando esta segurança é quebrada, seja acidentalmente, ou propositadamente, os resultados são altamente prejudiciais, por isso, a segurança dos BD é uma questão muito importante quando se desenvolve um projeto de política de segurança.

A base da segurança dos dados visa proteger a integridade dos mesmos, ou seja, garantir que eles somente sejam alterados, ou excluídos por pessoas autorizadas a efetuar tais operações (usuários fonte). Todavia, a segurança e a integridade dos dados não dependem somente das autorizações concedidas 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, como sendo uma forma de contrabando de dados, de maneira voluntária e executada por pessoas que têm acesso garantido aos referidos dados e praticam livremente essa ação.

O primeiro passo para a implementação de segurança de Banco de Dados requer a garantia do estabelecimento de uma política de privacidade e segurança, isso é, a definição do ambiente computacional que irá armazenar o dados – "Hardware e Software", bem como a definição do controle físico, humano e procedimental do acesso aos dados. Essa política irá definir o que deve ser feito e não como faze-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 alto grau de confiabilidade, a política de segurança. Quanto mais alta for essa garantia, mais difícil será quebrar a política de segurança.

As políticas de seguranças de Bancos de Dados devem levar em consideração três objetivos fundamentais:

- **Segredo –** Prevenir o acesso às informações por usuários não autorizados, como por exemplo: em um sistema de folha de pagamento, um empregado de nível inferior não deve ter acesso aos salários de seus superiores.
- **Integridade –** Evitar modificações das informações por usuários não autorizados a executar esse procedimento, como por exemplo: neste mesmo sistema de folha de pagamento evitar que um usuário altere o seu salário, sem que para isso esteja autorizado.
- **Disponibilidade –** Prevenir que alguma coisa ou fator impeça os acessos aos dados e às informações, como por exemplo, ainda nesse mesmo sistema de folha de pagamento os contra-cheques deverão ser impressos e entregues no prazo previsto.

2.1 – TIPOS DE BANCOS DE DADOS

Levando-se em consideração a forma de armazenamento e operacionalização os bancos de dados podem ser classificados em três categorias ou tipos:

- **Bancos de Dados Centralizados**
- **Bancos de Dados Descentralizados**
- **Bancos de Dados Distribuídos**

2.1.1 – Bancos de Dados Centralizados

Neste tipo de arquitetura de BD, todos os dados ficam armazenados e disponíveis em uma única unidade. Os serviços poderão ser executados nesta mesma unidade (processamento centralizado), ou os serviços serão realizados em diversas plataformas (processamento descentralizado/distribuído).Este tipo de arquitetura facilita bastante a segurança, uma vez que os dados são armazenados em um só local físico.

Todas as precauções a serem adotadas pelas políticas de segurança serão facilitadas nesta arquitetura de BD, desde o simples controles de aceso, até os mais eficientes sistemas de "backup" poderão ser executados de forma eficiente e segura.

Os sistemas que utilizam BD têm sido feito, tradicionalmente, de maneira centralizada. Desta forma, o banco é armazenado em um único computador, onde são acessados para serem executados. Neste tipo de arquitetura existe uma grande facilidade de controle de segurança e manutenção da integridade dos dados.

Apesar de todas as vantagens que possamos advir desta arquitetura, a centralização dos dados pode não atingir o principal objetivo dos mesmos que é a facilidade de acesso aos referidos dados, ou seja, tornar os dados mais 'facilmente disponível aos diversos usuários.

2.1.2 – Bancos de Dados Descentralizados

Neste tipo de arquitetura, o BD é dividido em partes, geralmente por setores ou áreas funcionais, tornando os dados mais facilmente disponíveis aos principais usuários dos setores correspondentes. Apesar de não ser exatamente um Banco de Dados Centralizado, a segurança dos dados é feita, basicamente, como no modelo de arquitetura centralizada, uma vez que o dado, mesmo não estando armazenados em um só lugar, cada área funcional é centralizada em um só local, o que facilita o controle de acesso aos dados de cada área.

Os bancos de dados descentralizados formaram as primeiras tentativas para a descentralização do processamento, tendo como principal objetivo atender a um maior número possível de usuários e diminuir o tempo de resposta aos "jobs" em processamento. A sua implantação necessita de uma rede de teleprocessamento, pois, as partes que constituem o banco de dados ficam residentes em cada nó dessa rede.

O surgimento e a posterior evolução da microinformática foram fatores que contribuíram para a implantação deste tipo de banco de dados, todavia, outros problemas tais como: a acessibilidade, a necessidade da corporatividade dos dados, o desempenho das redes e outros surgiram e fizeram com que esta arquitetura fosse gradativamente abandonada.

Como não podia deixar de acontecer, novos problemas no que diz respeito à segurança e ao gerenciamento deste tipo de arquitetura surgiram. Como os dados não estão presentes fisicamente em um mesmo local e podem estar espalhados em diversos pontos de uma rede, fica muito mais complicado o estabelecimento de competências, de nível de acessibilidade, de controle de transações, de confecção de cópias de "backup" e outros procedimentos de segurança.

Outro fator importante surge na possibilidade da duplicação dos dados em plataformas secundárias que se destinam a operar como "Work Station" (WS) e que por suas capacidade de armazenamento e de processamento, seriam capazes de conter grandes volumes de dados duplicados. É fácil de percebermos os

riscos que tais procedimentos podem ocasionar e a possibilidade real de ferirmos quase que a totalidade dos **requisitos fundamentais dos dados,** vistos no capítulo anterior.

Assim, gradativamente esta arquitetura foi sendo abandonada, mas a necessidade de se buscar uma solução que pudesse atender o desenvolvimento das empresas, buscando novos espaços e distribuindo-se territorialmente e, conseqüentemente, o aumento da demanda do processamento de dados, permaneceu e obrigou a criação de uma nova arquitetura para os bancos de dados.

2.1.3 – Bancos de Dados Distribuídos

Este tipo de arquitetura de banco de dados vem tomando destaque no mercado empresarial, pois, sendo uma variação mais moderna dos bancos de dados descentralizados vistos anteriormente, e quando tem um gerenciamento adequado e bem implantado garantem a operacionalidade em níveis bastante razoáveis.

Neste tipo de arquitetura, o BD é dividido em partes sem que se observe a divisão por setores ou áreas funcionais, tornando os dados mais facilmente disponíveis para todos os usuários de todos os setores. Apesar de não ser exatamente um Banco de Dados Centralizado ou Descentralizado, a segurança dos dados é feita, basicamente, como no modelo de arquitetura centralizada. A sua implantação também necessita de uma rede de teleprocessamento, pois, as partes que o constituem ficam residentes em cada nó dessa rede.

A vantagem em se ter um Banco de Dados Distribuído reside na vantagem de se definir as aplicações, com o compartilhamento total dos recursos – Hardware, Software, Dados e Informações – já que o sistema gerencia esses dados, mesmo que se encontrem distribuídos ao longo dos nós das redes, mantendo assim o controle dos dados e aumentando a operacionalidade do sistema, confiabilidade e a segurança dos dados, através da replicação (cópia operacional) das partes mais importantes do banco de dados em mais de um ponto da rede de teleprocessamento.

Podemos, também, ser mais eficientes através da adoção de um critério de particionamento e de replicação do banco de dados, de forma que os dados mais utilizados residam mais próximos do local onde serão utilizadas com maior freqüências.

O Sistema Gerenciador do Banco de Dados Distribuído (SGBDD) terá que definir meios e critérios de autorização para acesso aos dados, garantindo desta forma a segurança dos dados.

Dentre as principais funções de um SGBD Distribuído temos algumas que tratam da segurança dos dados, dentre as quais podemos citar:

- **Controle de Concorrência**
- **Controle de Integridade**
- **Controle de Acesso**

2.1.3.1 – *Controle de Concorrência*

O controle de concorrência que tem como objetivo a garantia que em toda a execução simultânea de um grupo de transações cada uma seja executada como se fosse a única presente no sistema. Em outras palavras, as transações não devem sofrer interferência que levem a anomalias de sincronização, como a perda a perda de consistência dos dados presentes no banco, o que acarretaria em acesso a dados inconsistentes.

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

Existem três tipos de controle de concorrência:

- **Técnica de Bloqueio –** esta técnica consiste no bloqueio do 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 –** esta técnica estabelece uma prioridade de execução de transações, executando-as serialmente como se fossem escolhidas por prioridades previamente estabelecidas.
- **Técnicas Mistas –** esta técnica tenta combinar as vantagens das técnicas de bloqueio e de pré-ordenação de forma que este tipo de controle de concorrência possa garantir o maior nível de segurança de acessibilidade aos dados, melhorando consideravelmente não só a operacionalidade como também os níveis de segurança do banco de dados.

2.1.3.2 – *Controle de Integridade*

Outra técnica utilizada pelos SGBD Distribuídos para garantir a segurança dos dados é o controle da integridade. Nesta técnica o controle de integridade dos dados é implementado não só nas partes parcionadas do banco de dados, como também com a visão do banco de dados geral. Assim o gerenciamento dos bancos de dados passa a ser executado não apenas por um único administrador e sim por um colegiado de administradores que envolvem os administradores locais e regionais, sob a coordenação do administrador geral do banco de dados.

Este tipo de arquitetura de bancos de dados passou a dividir os usuários em grupos pré-definidos o que facilita consideravelmente a determinação de competências, responsabilidades e acessibilidade. Assim podemos dividir os usuários em dois, com as suas respectivas subdivisões:

- **Usuários Sistêmicos**
  - **Gerentes de Sistemas**
  - **Administradores de Bancos de Dados – Geral, Regionais e Locais.**
  - **Gerentes de Projetos de Sistemas**
  - **Analistas de Sistemas**
  - **Programadores**

- **Usuários Gerais**
  - **Usuários Paramétricos**
  - **Usuários Casuais**
  - **Usuários Eventuais**

A divisão dos usuários em grupos e a definição de suas competências vieram suprir uma lacuna de segurança que não foi atendida pela arquitetura de bancos de dados descentralizados. Assim toda a problemática encontrada naquele tipo de arquitetura foi em parte solucionada, porém passou a exigir uma coordenação bastante rigorosa das atividades dos usuários e uma administração e gerenciamento da política de segurança voltada para as transações realizadas com os dados.

Não podemos acreditar que essa técnica não fique sujeita a ocorrência de falhas, pois elas podem ocorrer em dois níveis – "hardware e software" – tanto nos processadores locais, como nos

periféricos que armazenam os dados e, ainda, nas redes de comunicação de dados que dão suporte a essa arquitetura.

2.1.3.3 – *Controle de Acesso*

A última técnica utilizada na prevenção e garantia da segurança dos dados em um sistema de banco de dados distribuídos é a do controle de acesso que tem como objetivo a implementação de mecanismos que garantam esta segurança, deixando que os mesmos sejam manipulados somente por usuários previamente autorizados.

Esse controle restringe a acessibilidade, fazendo com que um grupo de usuários tenha acesso à somente determinadas partes do banco de dados. Assim sendo, o usuário terá acesso ao banco somente através da sua visão, ou nível. O sistema deverá oferecer também um mecanismo de concessão de privilégios, de forma que quando um usuário se "logar" ao sistema ele possa ser identificado, e o sistema verificará se o referido usuário possui os privilégios necessários à execução do acesso e em qual nível ele será permitido efetuar as suas transações.

Devemos levar em conta que controlar o acesso de usuários a um banco de dados consiste em assegurar que eles somente poderão realizar determinadas operações dentro de uma base de dados, se estiverem previamente autorizados a fazê-la. Esses controles são baseados no fundamento de que todos os usuários são previamente identificados e autorizados a realizar operações com os referidos dados.

As linguagens Stuctured Query Language (SQL) possuem comandos do tipo "Grant" e "Revoke" que tratam da concessão de privilégios de acessos aos dados. O primeiro fornece a um usuário os privilégios, enquanto o segundo possibilita que os privilégios sejam retirados em sua totalidade ou parcialmente.

Alguns princípios de controle de acesso nos permitem realizar um controle mais consciente e eficaz. O controle discriminatório consiste em dar a diferentes usuários diferentes tipos de acesso a diferentes objetos e dados, utilizando para isso os comandos disponíveis no SQL.

Atualmente o padrão SQL permite que nos possamos conceder quatro tipos diferentes de privilégios que podem ainda ser combinados para permitir o acesso totalmente diferenciado a cada tipo de objeto dentro de um banco de dados, são eles:

- **Insert –** permite a inserção de novos dados
- **Delete –** permite a remoção de dados existentes
- **Read –** permite a leitura dos dados
- **Update –** permite que os dados sejam alterados

Outro aspecto importante no controle do acesso aos dados baseia-se no conteúdo dos mesmos, isso é, mesmo que o usuário tente fazer algo que não seja correto, mas que ele tenha a permissão para isso, ele poderá esbarrar em certos "limites" também chamados de "visões".

Por exemplo, no sistema de folha de pagamento, anteriormente citado, um usuário que tente alterar seu próprio salário em valores quaisquer, pode esbarrar em uma visão que determina que o máximo que poderia ser alterado naquela tabela, por aquele usuário, com as suas permissões, é em um valor muito abaixo do que tentou fazer e, assim, teve o seu acesso barrado pelo nível em que foi previamente colocado.

Outro método importante de controle de acesso aos bancos de dados é o "**Acesso Mandatório Bel La Padula"** onde cada objeto do banco de dados recebe um nível de classificação que pode ser:

Ultra-secreto, Supersecreto, 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 bastante importante e interessante quando se fala em bancos de dados de qualquer tipo de arquitetura, é a técnica que trata de misturar e/ou codificar os dados para que, quando forem armazenados e/ou transmitidos por um meio de comunicação qualquer utilizado pelas redes de teleprocessamento, não permita que o banco se torne vulnerável a acessos indevidos e não autorizados, por meio de armazenamento e transmissão de bits inteligíveis. Essa técnica, chamada de **"CRIPTOGRAFIA"** é muito importante para a segurança dos bancos de dados, uma vez que eles permanecem armazenados por um longo período de tempo em meios de fácil acesso.

2.2 – SEGURANÇA NOS SGBDS ATUAIS – ANÁLISE COMPARATIVA

Passaremos agora a analisar comparativamente os principais Sistemas Gerenciadores de Bancos de Dados com relação aos aspectos funcionais de segurança.

Durante a análise desses SGBD's verificaremos que todos possuem uma ferramenta comum chamada SQL e, ainda, constataremos que cada um desses sistemas possui funcionalidades diferentes e tratam diferencialmente dos aspectos de segurança em seus aplicativos de manipulação dos dados.

Não pretendemos, e nem tampouco conseguiríamos, analisar todos os SGBD's existentes, assim tomamos por base os mais freqüentemente utilizados, tais como:

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

2.2.1 - Microsoft SQL Server 7.0 – Query Analyser

A atualização de versões dos diversos produtos da Microsoft é realizada através da aplicação de "Service Packs", assim resta-nos perguntar como descobrir qual a versão de SQL que se encontra instalada em nosso servidor. A resposta a esta pergunta poderá vir a partir de um comando SQL:

"SELECT @@VERSION"

A partir do número da versão obtida podemos descobrir qual o "Service Pack**"** utilizando a tabela abaixo:

VERSÃO	SQL	SERVICE PACK
6.50.201	SQL 6.5	Sem SP
6.50.213	SQL 6.5	SP1
6.50.240	SQL 6.5	SP2
6.50.258	SQL 6.5	SP3
6.50.281	SQL 6.5	SP4
6.50.415	SQL 6.5	SP5
6.50.416	SQL 6.5	SP5a
7.00.623	SQL 7.0	Sem SP
7.00.699	SQL 7.0	SP1
7.00.842	SQL 7.0	SP2
7.00.961	SQL 7.0	SP3

De posse do número da versão instalada, devemos nos preocupar com uma falha gravíssima que muitas vezes é considerada um convite a uma invasão ao SQL Server 7.0.

A definição de uma ***senha de caracteres brancos*** para a conta SA (System Administration) permitirá que sejam executadas todas as operações possíveis no seu banco de dados. Um dos maiores problemas é que durante a instalação padrão do SQL Server 7.0 não é exigido o uso de uma senha e, muitas vezes, seja por falta de uma conscientização de segurança, ou até mesmo por comodidade, acaba-se por utilizar uma ***senha de caracteres brancos*** (nula). Há ainda que se ressaltar que não basta somente definir uma senha para a conta SA ela tem que ser uma "senha forte", ou seja, ela deve conter um mínimo de oito caracteres e deve ser composta de números, de letras e de caracteres especiais (! - @ - # - $ - %).

Dessa forma, prevenimos a invasão do SQL Server 7.0, a partir de um ataque de quebra de senha por técnicas de "força bruta", ou por uso de "dicionários".

Para detectarmos quais as contas dos SQL Server 7.0 possuem senhas em branco, podemos realizar a seguinte consulta ao banco, através do **Query Analyser**, por exemplo:

"Use master Select name, password from syslogins where password is null by name"

Desta forma obteremos uma lista de contas que devem ter suas senhas implementadas e, ainda, que as mesmas sejam fortes.

Além das contas do SQL Server 7.0, devemos ter em mente que a interação com o Sistema Operacional se realiza através de uma conta de sistema e o nome utilizado por esta conta é **"SQLServices"** e a sua senha é considerada "fraca".

Uma implementação ideal seria não utilizar nome de conta padrão, renomeando esta conta de serviço para um outro nome e implementando uma senha extremamente forte, até porque ninguém a irá utilizar, exceto na hora de definição de seu uso como conta de serviço. Convém observar, ainda, que eventos de segurança obtidos no "log" do Windows NT irão se referir a tal conta quando ocorrer alguma coisa relacionado ao SQL Server 7.0.

Aproveitando que falamos do Windows NT, é interessante sabermos que o "log" de segurança do SQL Server 7.0 existe por natureza, mas que o seu estado padrão é não monitorar nenhuma ação. Para que se possa alterar esse parâmetro podemos utilizar a "stored procedure" **– sp_loginconfig.**

O SQL Server 7.0 possui as seguintes opções para a execução de uma auditoria:

- **NONE –** nenhuma informação é auditada
- **SUCCESS –** os acessos autenticados (logins) realizados com sucesso serão auditados
- **FAILURE –** as tentativas de "logins" com falhas serão auditadas
- **ALL –** todos os "logins" (com sucesso ou não) serão auditados

Essa auditoria será reportada tanto para o **SQL Server Error Log**, quanto para o Security Log do Windows NT.

Outra prática que podemos adotar é a utilização dos SQL Profiler que permite monitorar praticamente todos os eventos realizados no SQL Server 7.0, entre eles:

- **LOGIN FAILED**
- **LOCKING: DEADLOCK**
- **RPC: Completed**
- **OBJECT: Closed**
- **STORED PROCEDURE: Statement Starting**
- **SESSION: Disconnect**

Estas informações podem ser muito úteis para que possamos determinar **quem fez o quê e quando**, dentro do sistema.

Com relação à segurança dos arquivos dos bancos de dados, muitas vezes, por falta de interação entre o administrador da rede e do DBA(Data Base Administrator), ocorrem falhas nas definições das permissões de acessos aos arquivos dos SQL Server 7.0. Conforme já citado anteriormente, o SQL Server 7.0 interage com o Sistema Operacional através da sua conta de serviço e, na maioria dos casos, a definição das permissões para somente esta conta no diretório do SQL é suficiente.

Uma opção que podemos facilmente utilizar, quando usamos o SQL Server na plataforma Windows 2000, é o ***sistema de criptografia*** nativo desse sistema (**EFS – Encrypted File System)**. Dessa forma, podemos utilizar a conta de serviço do SQL para realizar a criptografia dos bancos de dados, impedindo que alguns usuários que não estejam autorizados consigam obter informações "em claro" após o acesso indevido ao referido banco.

Devemos nos lembrar, no entanto, das precauções que devem ser tomadas, como a necessidade de decriptografar os diretórios do SQL Server, antes de trocar o usuário que irá realizar a função de conta de serviço.

Abordando novamente o SQL Server 7.0 em si, muitas vezes, temos a idéia que o seu ambiente se encontra em "separado" do ambiente do Sistema Operacional, o que nem sempre é verdade. Como prova, temos como inclusão padrão no SQL Server a "extended stores procedure**" – xp_cmdshell.** Esta procedure permite realizar todas as operações que o usuário da conta de serviço possui ao utilizar um "pronpt" de linha de comando.

Por exemplo, se o usuário da conta de serviço possuir permissões de parar um serviço bastaria realizar o seguinte comando SQL, via Q*uery Analyser:* **execute xp_cmdshell 'net stop'**.

Desta forma, caso não seja extremamente necessário o uso desta procedure, é possível e necessário remove-la através do seguinte procedimento, via Q*uery Analyser:*

```
use master
sp_dropextendedproc 'xp_cmdshell'.
```

Outra boa prática de segurança que podemos adotar é a utilização de "views e stored procedures" para o acesso à informação, permitindo a restrição de acesso direto às tabelas e, em muitas vezes, melhorando a performance de uma consulta.

O SQL Server 7.0 é uma ferramenta bastante complexa que nos obriga a mantermo-nos sempre atualizados. Apenas como demonstração, procure no diretório do Windows (normalmente c:\WINNT) e no diretório TEMP os arquivos "**Setup.iss"** e **"sqlp.log" .**

Possivelmente você irá encontrar a senha do SA (System Administrator) armazenada em claro. Esta falha de segurança pode ocorrer durante o processo de instalação dos "Services Packs do SQL Server", quando utilizamos o método de autenticação padrão – "Standard Security".

Para evitarmos esse problema, devemos instalar o "Services Packs do SQL Server" utilizando o método integrado de autenticação, ou removendo destes arquivos temporários tais informações críticas.

O Manual de Segurança do MS SQL Server 7.0 descreve que a segurança deste SGBD é baseado no modelo de segurança do Windows NT, dessa maneira, passaremos a comentar resumidamente sobre alguns aspectos de segurança do Windows NT.

O SQL Server 7.0 possui dois modos para garantir a segurança no acesso ao servidor que são:

- **Windows NT Authentication Mode –** Modo de autenticação do Windows NT
- **Windows NT Mixed Mode –** Modo de autenticação mista do Windows NT

A segurança em um ambiente MS SQL Server 7.0 está intimamente relacionada: à segurança do Sistema Operacional no qual o Banco de Dados encontra-se instalado, com a configuração dos parâmetros de segurança do SQL e sua atualização de versão.

Trataremos, agora, separadamente, esses modos de segurança.

2.2.1.1 – *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/ou grupos permissões de acesso.

Quando o modelo de autenticação do windows NT é utilizado, o DBA permite que os usuários tenham acesso ao computador que está executando o SQL Server, garantindo a eles o direto 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/ou grupos de usuários, sem a necessidade da criação de contas de acesso para os mesmos usuários no SQL Server 7.0.

A concessão de acesso aos usuários e/ou grupo de usuários deverá ser da seguinte maneira:

- **Windows NT**

Os administradores devem criara contar de acesso para cada usuário, concedendo permissões de acessos ao SQL Server a cada um deles. Para os que já possuem contas basta conceder a permissão.

Após a criação das contas, podem ser criados grupos globais, onde os usuários serão agrupados de acordo com as 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 Server 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 o 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 deles são armazenadas em um arquivo de "log".

- **MS SQL Server 7.0**

O administrador do Banco de Dados deve conceder aos grupos locais criados no Windows NT permissões de acesso ao SQL. A permissão de acesso pode ser concedida a cada usuário separadamente, todavia, esse procedimento não é de fácil administração quando se tem grande quantidade de usuários.

2.2.1.2 - *Windows NT Mixed Mode*

Neste modelo os usuários também podem ser autenticados diretamente através do Windows NT, da mesma forma como era feito no Windows Authentication Mode. No entanto, os usuários deverão fornecer ao SQL um "**user number"** e uma **senha** que serão comparados com os que se encontram armazenados em suas tabelas de sistemas.

Este tipo de conexão é chamado de "***non-trusted conection"*** (conexão não confiável). Este sistema de conexão não confiável somente é recomendado quando o SQL Server 7.0 está instalado sobre o Windows 95/98.

Para que possamos garantir o acesso ao SQL Server 7.0 através de conexões não confiáveis, devem ser criadas contas individuais para cada um dos usuários diretamente no SQL Server 7.0.

2.2.2 – Oracle Server

No Banco de Dados Oracle, mais conhecido como Oracle Server, por se tratar de um Banco de Dados para múltiplas plataformas, a sua segurança não pode ser resguardada na segurança do Sistema Operacional em que foi instalado. Para isso, a instalação do Oracle segue uma política de depender o mínimo possível do Sistema Operacional e baseia-se na implementação de diversas medidas de segurança.

A primeira e principal medida é a alteração das senhas dos usuários padrão do banco. Usuários classificados como: ***"system"*** (que possuem senhas - ***manager***); ***"sys"*** (que possuem senhas – ***change_on_ install***); e ***"BDSNMP"*** (que possuem senhas – ***dbsnmp***) são classificados durante a instalação com estas senhas padrão e têm um alto nível de acesso ao banco de dados, fato que pode comprometer por completo a segurança do mesmo.

As tabelas dos sistemas, tais como as ***system***, devem ser protegidas contra os acessos dos usuários diferentes dos usuários de sistemas. A liberação de inclusão e de alteração dos dados nas referidas tabelas é um fato muito comum em ambientes de testes, onde programadores e/ou DBA tomam esta atitude para evitarem erros de aplicação por falta de privilégios. Todavia, esta prática em ambientes de produção é totalmente desaconselhável.

Devemos implementar diferentes perfis de usuários para diferentes tarefas no Oracle, tendo em vista que cada usuário/aplicação tem diferentes necessidades de acesso. Existe, ainda, a possibilidade de se proteger os perfis pó intermédio de senhas, o que é uma excelente medida. Além dessas medidas, o uso de cotas aumenta a restrição de espaço em disco a ser utilizado por usuários e/ ou aplicativos.

Para o acesso ao banco de dados, existem quatro formas de autenticação:

- **Através de um arquivo de senhas**
- **Autenticação herdada do Sistema Operacional** (usuário autenticado previamente S.Op.).
- **Arquivo de senhas do Sistema Operacional**
- **Autenticação nativa do Banco de Dados**

As três primeiras vão herdar a confiabilidade do Sistema Operacional, o que pode vir a ocasionar problemas de segurança. A política correta baseia-se sempre na confiabilidade do banco de dados, autenticado somente por ele e implementando-se um correta política de senhas. Tal método de identificação consta na "view – **V$SYTEM_PAREAMETER".**

Outra medida interessante seria realizarmos a alteração da porta de serviços padrão, com o intuito de dificultar a identificação da funcionalidade dos ativos do banco de dados, por meio de usuários mal intencionados.

A instalação padrão do Oracle prevê o acesso ao banco de dados através da porta "**1521".**

Sempre que possível, é importante executarmos testes de análise das tabelas e dos índices, com o intuito de verificarmos a estrutura das mesmas, para prevenirmos falhas de inconsistências e que de performance.

Os comandos abaixo são utilizados para efetuarmos as análises das tabelas:

ANALYZE TABLE (nome da tabela) ESTIMATE STATISTICS
e
ANALYZE TABLE (nome da tabela) VALIDADE STRUTURE

Os comandos abaixo são utilizados para efetuarmos as verificações dos índices:

ANALYZE INDEX (nome do índice) ESTIMATE STATISTICS
e
ANALYZE INDEX (nome do índice) VALIDADE STRUTURE

Devemos tomar cuidados com tais análises, pois elas oneram a performance do sistema. Na maioria dos casos, recomenda-se que a análise seja executada por amostragem (apenas analisarmos parte das tabelas e índices).

A auditoria do sistema, aliada ao uso de "*triggers*" torna-se indispensável para mantermos o sistema sempre otimizado e resguardado de acessos indevidos.

Outra medida importante, para qualquer a garantia dos bancos de dados é a implementação de uma política de "backup" que contemple a rotação dos "arquivos de log" e que este "backup" tenha o seu armazenamento "off-site".

Para ambiente que necessitem de alta disponibilidade, existe ainda uma opção do Oracle que prevê redundâncias do banco de dados, utilizando-se dos conceitos de replicação, valendo-se de recursos computacionais de terceiros.

Além dos sistemas auxiliares para os bancos de dados e seus aspectos de proteção, existem ferramentas adicionais que incrementam a segurança do Oracle Server, possibilitando um ambiente multi-plataformas de maior escala. Tais ferramentas dividem em dois grupos: as gratuitas e as pagas.

Entre as ferramentas gratuitas, existem dois produtos em particular que são vendidos juntamente com a versão básica do Oracle Server. Estes produtos são:

- **Oracle Enterprise Manager (OEM)**
- **Oracle Security Server Manager (OSS)**

O **Oracle Enterprise Manager (OEM)** é um conjunto de utilitários que são disponibilizados em uma interface gráfica em modo usuário (GUI) provêm meios para gerenciar uma ou mais bases de dados de um único computador. O **OEM** é composto por:

- **Um conjunto de ferramentas Administrativas;**
- **Um monitor de eventos que pode ser configurado para inspecionar situações específicas em sus base de dados;**
- **Um agendador de tarefas para executar tarefas de manutenção, em horários previamente definidos;**
- **Uma interface gráfica para o Recorvery Manager Tools.**

O **Oracle Security Server Manager (OSS)** pode ser utilizado para implementarmos uma estrutura mais complexa de segurança para os dados considerados mais sensíveis, com os seguintes aspectos:

- **Autenticação dos usuários, através de credenciais eletrônicas;**
- **Assinatura digital;**
- **Single Sing On (SSO)**

Todas essas opções são implementadas em modo "stand-alone" em outras palavras, não é necessário que tenhamos produtos de terceiros, como por exemplo: *"kerberos"*, ou qualquer outro produto do Oracle tal como: o "***Advancet Networking Option"*** para fazermos uso do **OSS.**

Entre as ferramentas pagas do Oracle podemos citar:

- **Trusted Oracle –** provê a segurança em diversos níveis (**MLS – Multi Level Security)**
- **Advanced Networking Option –** utilizado para encriptar todos os dados trafegados no SQL*Net ou no Net*8, entre o cliente e o servidor.
- **Oracle Application Server –** anteriormente chamado de "*Web Application Server"* ou *"Internet Aplication Sever"* que é utilizado para a integração com aplicações baseadas na WEB.

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 têm autorização, além de controlar o uso do espaço e dos recursos disponíveis, fazendo também a auditoria das ações dos usuários.

Existem duas categorias de segurança do Oracle:

- **Segurança do Sistema;**

- **Segurança dos Dados.**

2.2.2.1 – *Segurança do Sistema*

A **Segurança do Sistema** é aquela em que os mecanismos de segurança controlam os acessos ao banco de dados em nível de sistema, ou seja, controlam a validação do nome e a senha do usuário; os espaços disponíveis em discos para criação e controle do objeto; o limite dos recursos; a auditoria dos recursos; e as operações que o usuário pode executar.

2.2.2.2 - *Segurança dos Dados*

A **Segurança dos Dados** é aquela em que os mecanismos de segurança controlam os acessos aos bancos de dados em nível de objetos, ou seja, criar privilégios e restrições aos acessos às informações. Isso é feito concedendo um privilégio apropriado a cada um dos usuários, para um determinado objeto.

A operacionalidade e a confidencialidade no SGBD Oracle está baseado nos seguintes parâmetros:

- **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"*.

- **Controle de Acesso Discriminatório –** faz a restrição dos usuários permitindo a realização de determinadas operações e de acesso a determinados objetos do banco de dados através da concessão de privilégios.

- **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 somente poderá acessar os objetos cuja informação não seja confidencial no seu nível.

2.2.2.3 – *Auditoria*

A auditoria é feita pela gravação das operações executadas no banco de dados e os respectivos usuários que as executaram, com objetivo de gerar um "*arquivo de auditoria"* que possa ser analisado a qualquer momento, para detectar ameaças de violação 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 sistema.

2.2.2.4 – *Encriptação no Banco de Dados*

Cada banco de dados no Oracle é armazenado de uma forma codificada que somente poderá ser decifrada com o uso de um software específico e a chave de decodificação correta.

2.2.3 – IBM DB2

O banco de dados IBM DB2 não é um banco muito conhecido e nem tão pouco utilizado em plataformas "descktop", todavia em grandes empresas e em ambientes de médio e de grande porte ele é muito utilizado, principalmente nos ambientes AS 400 de fabricação da IBM.

O motivo que levou à sua utilização pelas grandes empresas é o fato de que ele é um gerenciador eficiente e tem um custo razoável e que a sua operação é praticamente automático, quando corretamente configurado, pois possui 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 tarefa de 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 e isso se tornará um exercício de paciência, pois, o centro de controle DB2, onde trabalhamos com o SQL, executa os comandos um a um, isto é, você digita uma linha e ele executá-la, repetindo éster procedimento até o final do seu comando.

2.2.3.1 – *Segurança no IBM DB2*

Como em todos os bancos de dados anteriormente pesquisados, a segurança no IBMDB2 se limita somente a processos de autenticação e autorização de usuários, combinados a sistemas de segurança externos (Sistemas Operacionais).

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

Existem dois tipos de autorizações no DB2:

- **Os privilégios –** que define uma permissão simples ao usuário, isto é, ele pode criar e acessar recursos do seu banco de dados;

- **Níveis de autorização** – dizem respeito ao controle de privilégios de grupo, atribuindo a um usuário, dentro deste grupo, o poder de atribuir 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 de bancos de dados e o seu administrador esteja sempre atento às possíveis falhas e realize auditorias constantes, para preservar a integridade do mesmo.

2.2.4 – Microsoft ACCESS

Não é difícil perceber a intenção da ferramenta Microsoft ACCESS como uma solução de SGBD desenvolvida para o armazenamento e o gerenciamento de pequenos volumes de dados, cujo principal objetivo é ser uma ferramenta de fácil utilização. Uma de suas virtudes é a capacidade de integração com outras soluções e produtos.

O fato de ser uma ferramenta de fácil utilização, não implica que tenha recursos limitados. Muitas vezes as limitações surgem pelo fato de um pequeno banco de dados possuir variáveis completamente distintas de um banco de dados robusto no que se refere a controle, volume, gerenciamento e segurança.

Como o Microsoft ACCESS atende, em sua maioria, às pequenas e médias aplicações, não poderá ser avaliado ou comparado com SGBDs para aplicações mais robustas. No entanto, devido a sua fácil utilização e capacidade de integração, acaba tornando-se uma das soluções prediletas para os que desenvolvem aplicativos para WEB que precisam manipular pequenas quantidades de dados.

É necessário muita cautela ao montarmos um ambiente WEB integrado com Microsoft ACCESS. Muitos aspectos devem ser considerados, uma vez que este não é o foco principal desta solução. Algum deles podem ser observados a seguir,onde passamos também a descrever algumas recomendações a serem observados pelos desenvolvedores de aplicações em ACCESS:

- Sempre que possível manter o Banco de Dados em um diretório não público;

- Quando manipuladas informações sigilosas, como senhas de usuários, devemos tratar a criptografia antes da inserção dessas informações no banco de dados;

- Sempre que possível realizar a conexão ao banco de dados por "**Open Database Connectivy"** (ODBC);

- Num sistema de arquivos "NTFS" em plataforma Windows, alterar as permissões de acesso aos arquivos do banco de dados de modo a impedir o acesso aos usuários não autorizados;

- É de extrema importância tratarmos a consistência das informações em variáveis antes de repassá-las ao banco de dados. Um dos maiores vilões da segurança para o ACCESS é a integração com funções do Visual Basic (VB), onde um usuário poderá executá-las durante o acesso aos dados (realização de umas consulta);

- Quando utilizarmos: formulários, relatórios e consultas, nativos do ACCESS, para gerenciarmos informações em tabelas, é recomendável mantê-los em um arquivo (Front-end) separado do arquivo de tabelas (back-end). Desta forma, o arquivo de gerenciamento poderá ser movido sem que haja necessidade de movimentação dos dados armazenados na tabela;

- Converter o Arquivo "Front-end" para o formato Microsoft Database Executable (MDE), de modo a garantir a propriedade intelectual das estruturas e códigos de programações;

- Restringir o acesso de usuários ao banco de dados baseado no arquivo de grupos de trabalhos do ACCESS. O uso de senhas no acesso ao banco de dados ainda encontra-se mal implementada, o que permitiu o desenvolvimento de programas que extraem a senha diretamente do banco de dados, sem que tenhamos, ao menos, o trabalho de quebrarmos estas senhas;

- É importante a criação de um novo arquivo de grupo de trabalho diferente do arquivo padrão criado na instalação do banco. O novo arquivo caracteriza-se pela criação de uma chave única de identificação, impedindo assim a sua duplicação e a possível manipulação de permissões;

- Quando criptografarmos o banco de dados através do Microsoft ACCESS é padrão que as informações fiquem gravadas sem criptografia no arquivo, deixando-as frágeis mesmo após a implementação dos diversos recursos de segurança.

Quando não são levados em consideração os aspectos de segurança do banco de dados, não só as informações nele contidas ficam comprometidas, como também todos os blocos que compõem a solução, como por exemplo: *"Um sistema WEB integrado a um banco de dados sem informações relevantes pode ter um sistema operacional controlado por invasores que usem simples funções de programação"*. Para protegermos um sistema é necessário atenção a todos os blocos que o formam, incluindo os aparentemente menos relevantes.

CONCLUSÃO

O problema de segurança envolve aspectos tanto políticos quanto técnicos.

A escolha correta de um Sistema Gerenciador de Banco de Dados tem, obrigatoriamente, que passar por uma análise minuciosa não só com relação aos aspectos operacionais que este gerenciador oferece, mas também em relação às características de segurança que ele possibilita.

Absolutamente não é uma tarefa simples, todavia, da adoção de critérios rígidos e bem formulados é que resultará em níveis de segurança maiores ou menores. As empresas modernas não podem mais arriscar seus dados e informações, deixando que eles estejam desprotegidos pela adoção de um SGBD que não ofereça os requisitos necessários aos níveis de segurança desejados.

Como podemos ainda observar, a maioria dos Sistemas Gerenciadores de Bancos de Dados compartilha a garantia da segurança com os Sistemas Operacionais, fazendo com este aspecto passe a ser um assunto tratado de forma integrada entre esses dois níveis e gerenciado pela integração desses dois sistemas.

Obviamente, em caso de má integração ou mesmo de falha na observação dos aspectos de segurança de qualquer um dos dois sistemas, poderá ocasionar “brechas” e falhas que somente serão percebidas por uma análise criteriosa por parte dos DBA.

Os processos de auditorias são ferramentas poderosas na análise e na manutenção dos níveis de segurança pretendidos, todavia, a sua realização em intervalos de tempo muito grandes, poderá deixar os dados a descoberto por longos períodos o que não é admissível em qualquer empresa.

Conforme podemos observar, a partir dos fatores acima relatados, é de extrema importância a analise comportamental dos Sistemas Operacionais com relação aos aspectos de segurança, conforme passaremos a estudar a seguir.

CAPÍTULO III

SEGURANÇA DOS SISTEMAS OPERACIONAIS

CAPÍTULO III
SEGURANÇA DOS SISTEMAS OPERACIONAIS

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" dos Sistemas Operacionais: o que elas são, de onde vêm e o que nos podemos 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 de uma política de segurança confiável, dentro de uma empresa, para depois aplicarmos esse esquema dentro de cada um exemplo abordado de Sistema Operacional.

3.1 - BRECHAS

A "brecha" nada mais é do que um "bug" (uma falha) em qualquer hardware e software, ou diretiva de segurança que expõe as vulnerabilidades do Sistema Operacional, ou de sua rede de Comunicação de dados, permitindo acesso não autorizado, comprometendo os sistemas e as ferramentas que compõem um ambiente computacional, dentro as quais podemos citar: Roteadores e os Firewalls.

Com o desenvolvimento da Internet em todo o 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 o uso dessas brechas em proveito pessoal.

Se não tivermos intenção de deixarmos a nossa rede totalmente exposta, devemos ficar atentos ao mundo externo, atualizando-nos quando da divulgação das novas brechas que vêm sendo descobertas a cada dia, para que possamos efetuar a posterior prevenção.

3.1.1 - Como Surgem as Brechas

As brechas não aparecem sozinhas, elas são descobertas por usuários que pesquisam constantemente os ambientes computacionais, tentando descobrir falhas dos sistemas, para dessas falhas tirarem proveito ou não. O grupo constituído de "Crackers e Rackers" e das equipes de segurança formadas pelos fabricantes são os principais tipos de usuários que descobrem essas brechas.

Dependendo de que as descubra essas informações, elas podem ser distribuídas ao público de diferentes maneiras:

- **Crackers -** se a descoberta foi feita por um "cracker" a primeira notícia que recebemos é da invasão de um grupo de servidores invadidos utilizando a brecha encontrada;

- **Hackers -** se a descoberta foi feita por um "hacker" a notícia que recebemos é da descoberta de uma brecha acompanhada de recomendações em boletins de segurança, por intermédio de revistas e jornais especializados, ou pela própria Internet;

- **Equipes de Segurança -** se a descoberta foi feita por uma equipe de segurança de um fabricante qualquer, esta informação sempre é a última a chegar na mídia, pois já virá acompanhada da solução.

3.2 – POLÍTICAS DE SEGURANÇA DOS SISTEMAS OPERACIONAIS

A implementação de uma Política de Segurança confiável, está diretamente relacionada à criação de usuários. Temos que ter em mente, antes da criação desses usuários e/ou grupos de usuários, quais serão os recursos computacionais e da rede de comunicação de dados (arquivos e diretórios) eles terão acesso.

O Administrador da Rede deverá ter o controle total sobre esses usuários e sobre os recursos computacionais que serão utilizados por eles. Para definir as restrições e os privilégios que serão aplicados aos usuários, o Administrador da Rede deverá conhecer perfeitamente as funções e as necessidades de cada um dos usuários, no contexto geral da empresa.

Dentre as definições dos privilégios e das restrições está o compartilhamento dos recursos da rede, como por exemplo: "em um sistema centralizado, definiremos quais as pastas e/ou arquivos serão compartilhadas e quais os usuários terão as devidas permissões de acesso a esses recursos".

Fica a critério do administrador da rede qual à medida que ele irá adotar para realizar a proteção dos arquivos mais importantes dentro de sua rede, se ele vai validar o acesso do usuário; se vão colocar senhas para acesso a uma determinada pasta, com a validação inicial do usuário(log); ou, dependendo da importância do arquivo final, ele acrescentará mais uma senha para permitir o acesso (acesso mandatório).

Além da colocação excessiva de senhas, o arquivo poderá também ser criptografado, fazendo com que, além da senha de acesso, haja uma chave especial de acesso que se encarrega de descriptar o arquivo, assim que ele chega ao seu destino. Assim, caso o arquivo seja interceptado no meio de uma transmissão, não passará de um punhado de letras sem o menor sentido para aquele que o interceptou.

Todavia, o mais importante de tudo, independente dos níveis de proteção para um arquivo/conjunto de arquivos é que eles sejam administrados dentro da empresa, ou local onde estejam sendo implantadas as políticas de segurança. Todos nos devemos ter em mente que a melhor medida de segurança possível e a velha e boa senha. Ela deverá ser bem escolhida e poderemos seguir pequenas e eficazes regras de criação que aconselharemos mais adiante.

Outro fator que devemos levar em consideração é o fato de que não importa o nível de segurança que tivermos, pois poderemos sofrer as conseqüências de uma invasão, e se isso acontecer o que devemos fazer?

Primeiramente devemos verificar o que foi danificado, ou perdido e restaurarmos aquilo que pudermos restaurar, através das últimas cópias de segurança (backup) que dispusermos. Por isso, uma política de "backup" deverá ser implementada dentre os usuários de um ambiente computacional, adotando boas rotinas de "backup"o que garantirá que os nossos dados estejam sempre atualizados e preservados, respondendo a perguntas razoavelmente simples, tais como:

- **Periodicidade –** de quanto em quanto tempo esse backup deverá ser feito?
- **Arquivos –** quais serão os arquivos/pastas a serem copiados?
- **Ferramentas –** como ele será feito?
- **Meio Físico –** que meio físico deverá conter as cópias de segurança?

As respostas a essas simples perguntas nos dará a garantia de que teremos maneiras eficientes de recuperarmos nossos arquivos, caso ocorram ataques às nossas empresas.

Por mais que nós (Gerentes de Redes, Administradores de Bancos de Dados, Gerentes de Centros de Processamento, etc) alertemos aos nossos usuários para com os perigos dos vírus computacionais, sempre irão existir aqueles usuários que pensarão que isso nunca irá acontecer com eles, e trarão para o local de trabalho, ou levarão para casa aquele disquete de procedência duvidosa, ou mesmo abrirá aquele "e-mail" do amigo com o pensamento – "ele é meu grande amigo e nunca me mandará um vírus" – e então era uma vez uma rede de computadores.

Por isso, devemos: manter o "anti-virus" de nossas empresas atualizados; verificar constantemente os boletins de segurança existentes na Internet; e ler revistas especializadas no assunto, pois elas sempre trazem notícias sobre 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 simples e barata e que requer um investimento significativo.

Geralmente quando não ocorrem situações de grandes danos e de perdas e/ou violação dos dados, esse investimento parece que foi feito em vão, todavia, quando este investimento não é realizado e ocorrem grandes prejuízos por invasões, as perdas na maioria das vezes são incalculáveis. Pois isso, o responsável pela informática dentro de uma empresa deverá saber como mostrar a todos que a segurança da informação é uma coisa que afeta a todos e todos deveremos ter as mesmas preocupações e responsabilidades.

3.3– CRITÉRIOS DE AVALIAÇÕES DE SEGURANÇA DOS SISTEMAS OPERACIONAIS

Os Sistemas Operacionais estão classificados, segundo o nível de segurança apresentado, em quatro categorias: **A, B, C, D,** ordenados de maneira hierárquica crescente, com a maior divisão (**A**) reservada aos Sistemas que oferecem maior nível de segurança.

Nas divisões **C** e **B** existem subdivisões conhecidas como classes as quais também estão ordenadas hierarquicamente.

A seguir faremos um resumo das divisões e classes dos critérios de avaliação dos Sistemas Operacionais:

3.3.1 - Nível de Segurança D – Proteção Mínima

Este nível é atribuído aos sistemas operacionais que não possuem nenhuma ferramenta ou alguns tipos de capacidade de garantir a segurança em nenhum aspecto. Este tipo de sistema é muito encontrado em ambientes e plataformas monousuário (MS DOS, PC-DOS, System 7.X, etc);

3.3.2 - Nível de Segurança C1 – Proteção Arbitrária

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidade de garantir a segurança em aspecto mínimos sem grandes valores de segurança. O TCB de um sistema desta classe satisfaz as exigências de segurança discricionária, separando os usuários dos dados. Ele incorpora alguns tipos de controle, capazes de reforçar as limitações de acesso numa base de dados individual. Isto é, ele foi criado de forma que, ostensivamente, permita aos usuários a capacidade de proteger o projeto ou as informações privadas e impedir que outros usuários tenham uma leitura acidental, ou a destruição dos seus dados. O ambiente de classe **C1** deve ser o de usuários cooperando entre si e processando dados no mesmo nível.

Para a utilização do Sistema Operacional são necessários o uso de senhas e de contas pessoais, onde o arquivo da senha é obtido por qualquer usuário. Neste grupo encontramos os sistemas das antigas plataformas UNIX e do Sistema XENIX. Conceitualmente o Sistema Windows NT está neste nível de segurança, pois, apesar do arquivo de senhas estar em método criptografado, já foram encontradas várias ferramentas e programas de descriptografia deste arquivo.

3.3.3 - Nível de Segurança C2 – Proteção de Acesso Controlado

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança em um nível médio, com alguns aspectos complementares de segurança, onde o arquivo de senhas é oculto aos usuários e utilizam um método forte de criptografia de dados.

Os Sistemas desta classe reforçam o controle de acesso descricionário, de forma mais precisa do que os sistemas da classe **C1**, tornando os usuários responsáveis individualmente por suas ações através de procedimentos de "logins", incluindo a capacidade de realizar auditoria de segurança em eventos.

3.3.4 – Nível de Segurança B1 – Proteção de Segurança Selada

Este nível é atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio, todavia o aspecto que o diferencia do nível C2 é a sua capacidade de armazenamento de todos os "logins" de acesso ao sistema por um tempo mínimo de 2 anos.

Os Sistemas da classe **B1** devem possuir todas as características exigidas para os Sistemas da classe **C2,** além do que, devem estar presente: uma exposição informal do modelo do projeto de segurança; a classificação dos dados; e o controle obrigatório do acesso aos usuário e aos objetos nomeados. Deve ainda existir uma capacidade de exportar informações de forma Selada (criptografada).

3.3.5 – Nível de Segurança B2 – Proteção Estruturada

Este nível é atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio, todavia o aspecto que o diferencia do nível B1 é a sua capacidade de armazenamento de todos os "logins" de acesso ao sistema por um tempo mínimo de 7 anos.

Nos Sistemas da classe **B2** o TCB se baseia em um modelo de projeto de segurança formal, claramente definido e documentado, exigindo que o esforço no controle do acesso discricionário e obrigatório encontrado nos sistemas da classe **B1**, seja estendido a todos os usuários e objetos de dados.

O TBC deve ser cuidadosamente estruturado dentro dos elementos de proteção: perigosa "arriscada" e as não perigosas. A interface do TBC é bem definida e o seu desenho e execução o torna apto a ser submetido a testes bem mais minuciosos e revisões mais completas.

Os mecanismos de autenticação são mais reforçados, as facilidades de gerenciamento, altamente confiáveis, são fornecidas sob a forma de apoio às funções de administrador e operador de sistemas, assim como são impostos controles rigorosos de configuração.

O sistema é relativamente resistente às penetrações.

3.3.6 – Nível de Segurança B3 – Propriedades de Segurança

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança em um nível bastante alto.

O TBC da classe **B3** deve satisfazer as exigências do monitor de segurança, de forma que ele possa medir todos os acessos de usuários aos objetos de dados, além disso, ser razoavelmente imune às invasões e suficientemente pequeno para que possa ser submetido a análises e testes.

Para que possa satisfazer estes requisitos, o TCB foi estruturado para excluir todo código não essencial ao reforço da segurança, com o uso significativo de métodos de engenharia de sistemas, para o seu projeto e o seu desenvolvimento, visando minimizar as suas complexidades.

Um módulo de Administrador de Segurança é mantido, os mecanismos de auditoria são estendidos aos eventos, com aplicação de avisos de segurança e procedimentos de restauração do sistema são exigidos.

Este tipo de Sistema Operacional é altamente resistente a ataques e penetrações.

3.3.7 - Nível de Segurança A – Desempenho Verificado

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança total dos sistemas, não apresentando falhas de segurança. Muitos autores acreditam que uma das poucas plataformas capaz de ter tal nível de segurança estaria no NSA e não existe no mundo, pelo menos que se conheça, máquina idêntica a esta.

Os Sistemas da classe **A** são funcionalmente equivalentes aos sistemas da classe **B3**, na medida em que não são acrescentadas características novas em sua arquitetura, ou exigências de planos de ações.

A característica que distinguem os sistemas desta classe é a análise derivada da especificação formal do desempenho, o emprego de técnicas de verificação e o alto nível de segurança resultante da forma correta com que o TCB for implementado.

Esta segurança é progressiva por natureza, começando com um modelo formal do projeto de segurança e uma especificação formal de alto nível do desempenho. De acordo com o seu desempenho ostensivo e da análise do TCB exigida para os sistemas da classe **A**, requer-se um gerenciamento mais rígido da validação dos usuários e os procedimentos de segurança são estabelecidos para a distribuição segura dos sistemas para os sites.

3.4 – ATUALIZAÇÕES DOS SISTEMAS OPERACIONAIS

A maneira mais correta de garantir o uso de um Sistema Operacional segura é mantê-lo atualizado. As atualizações são pequenos arquivos, se levarmos em consideração o tamanho total do Sistema, que contém correções de "brechas e bugs" e leva ao aprimoramento dos aspectos de segurança dos sistemas.

Para cada Sistema Operacional existem caminhos diferentes para encontrar as suas atualizações, como por exemplo: as atualizações do Windows 98/ME podem ser encontradas na página do Windows Update (windowsupdate.microsoft.com) ou em Cds que acompanham algumas revistas especializadas; já para o Windows NT/2000 as suas atualizações podem ser encontradas na própria página da Microsoft (**www.microsoft.com/windows/nt**) com o nome de "Server Pack); para o LINUX encontramos as suas atualizações na página do seu distribuidor da sua versão do LINUX, ou nas próximas versões do Cd.

3.5 – ANÁLISE DO DESEMPENHO DE SEGURANÇA DOS SISTEMAS OPERACIONAIS

A seguir passaremos a fazer uma análise sucinta do desempenho de segurança de alguns dos Sistemas Operacionais mais utilizados.

3.5.1– Sistema Operacional LINUX

Criado pelo universitário finlandês LINUS TORVALDS, em 1991, o Sistema Operacional LINUX é atualmente utilizado por grandes empresas, principalmente em aplicações ligadas a Internet.

A segurança no LINUX, assim como em qualquer outro Sistema Operacional Unix, deve ser vista de uma maneira diferente ao que vemos os Sistemas Windows. No LINUX um administrador deve se preocupar em saber quais são os problemas "bugs" existentes em toda a base de software instalado. Tais problemas poderão facilitar o acesso indevido de usuários maliciosos a todo o sistema.

Discutiremos a seguir, alguns tópicos importantes relacionados à segurança deste moderno Sistema Operacional.

3.5.1.1 – Controle de Acesso

O sistema de gerenciamento de arquivos do LINUX permite restringir o acesso aos arquivos e aos diretórios, associando a eles um conjunto de permissões e de privilégios. Essas permissões determinam quais são os arquivos que o usuário poderá ler e/ou manusear. Cada usuário assume um ou mais papéis com relação aos arquivos:

- **Proprietário ou Usuário:** o usuário é o dono do arquivo (geralmente o seu criador). O proprietário é que define as permissões de acesso ao arquivo.
- **Grupo:** o usuário pertence a um grupo de usuários relacionados ao arquivo. Neste caso, o arquivo poderá ser controlado por diversas 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 (consultar)
- **Escrita:** Permite que o usuário modifique o conteúdo de um arquivo (alterar)
- **Execução:** Permite que um usuário execute um programa e realize buscas em um diretório.

Mostraremos, agora, como são representadas as permissões em um arquivo:

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

Os comandos acima podem nos mostrar os atributos dos arquivos e diretórios (tamanho, data e hora da última modificação), seu proprietário, a que grupo está relacionado e as suas permissões. As permissões de leitura, escrita e execução são representadas respectivamente pelas letra "**r, w, x**" . Todavia quando uma permissão é negada, isso passa a ser 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 – diretório **L** – link "**-**" – para outros arquivos

A segunda coluna corresponde aos privilégios do proprietário do arquivo, e neste caso, ele tem permissão de leitura e de gravação sobre o arquivo de nome **TEXTO.TXT.**

A terceira e a quarta coluna correspondem, respectivamente, aos privilégios do grupo a qual este arquivo está relacionado e os outros usuários do sistema. Eles possuem apenas permissão de leitura sob o arquivo de nome **TEXTO.TXT.**

3.5.1.2 – *Segurança de Senha*

A segurança de senha do LINUX é confiável quando ela é implementada corretamente. Além de educar os seus usuários obrigando-os a criarem senhas difíceis de serem adivinhadas, o administrador deverá utilizar utilitários preventivos de senha, sombreamento de senhas e empregar as técnicas de 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 um

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 outra senha.

No sistema LINUX as informações dos usuários são guardadas no arquivo "**passwd**" localizado no diretório. Esse arquivo contém: nomes de "logins"; nomes dos usuários e suas senhas (criptografada).

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

3.5.1.3 – *Segurança de Conta Root*

A Conta "Root" (raiz) é uma conta administrativa especial que concede acesso irrestrito a todo o sistema. A Conta "Root" corresponde a do administrador no Windows NT e a do supervisor no NOVELL.

Esta conta poderá executar operações irreversíveis ao sistema, por isso é aconselhável utilizá-la somente quando for absolutamente necessário, como por exemplo: configurar um dispositivo, ou instalar um programa.

A existência de uma conta privilegiada pode ser considerada como uma ameaça ao sistema. Por possuir controle total do sistema, a "conta root" é o principal alvo dos "crackers", se a "conta root" for comprometida, toda a nossa rede também estará.

A segurança do sistema inicia-se no movimento da instalação do LINUX, quando é solicitada a configuração da senha de raiz. É verdade que distribuições, como o "**Red Hat Linux**" forçam a atribuição de uma senha antes da primeira inicialização. Todavia, o **LINUX SLACKWARE** permite que se efetue um "login" de "root" sem uma senha quando a instalação está completa. Torna-se, então, uma obrigação nossa a configuração desta senha.

No entanto, um "cracker" nem precisa efetuar "login de Root", apenas adquirir privilégios dele. Para isso o "cracker" se aproveita de "bugs" dos programas que precisam ser efetuados como "root". Quando o programa é atacado, concede, aos seus atacantes, os privilégios de "root".

Por isso, é importante manter-se atualizados sobre os surgimentos de novas falhas e as suas correções.

3.5.1.4 - *Serviços*

O Sistema Operacional LINUX possui alguns serviços que podem deixar o seu sistema vulnerável a ataques, ainda mais se esses programas estiverem conversões desatualizadas. Quando o seu computador é ligado, esses serviços podem ser iniciados pelo programa "**inetd"** ou pelos arquivos existentes dentro do diretório de inicialização do LINUX, chamados "**RC.d**".

Cabe ao administrador do sistema verificar se esses serviços são realmente necessários à sua rede e, caso contrário, desabilitá-los. Caso haja necessidade de alguns desses serviços, que ele utilize sempre a versão mais atualizada destes softwares.

Vejamos como se comportam alguns destes serviços:

- **Telnet –** este é um serviço que permite ao usuário não só efetuar "logins" em um "host" remoto, como também possibilita a execução de comandos neste "host".

Exemplo: uma pessoa na cidade "A" poderá acessar a uma máquina na cidade "B" e executar programas na máquina da cidade "B", como se ela estivesse nessa cidade.

O **Telnet** pode ser usado de inúmeras maneiras para atacar e/ou colher informações importantes de um "host" remoto. Contudo, se o administrador pretende fornecer aos seus usuários acessos de **Telnet**, ele deverá estar atento 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 deste aplicativo irá cortar a conexão caso o nome do 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 desta forma dar a um "cracker" mais uma chance de se conectar.

- **Finger –** este é um serviço comum para os Sistemas Operacionais UNIX. Ele fornece informações importantes sobre os usuários (logins; 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 do **Finger**, chamado de "fingerd", quando recebe uma solicitação de algum usuário, seja ela local ou remota, encaminha as informações do usuário alvo que estão atualmente disponíveis. Por isso, muitos administradores não oferecem este serviço aos seus usuários.

Existem outros serviços cuja segurança deixa muito a desejar, como o "**LPD, APN, DHCPD, NFS e SMB**" que se não estiverem sendo utilizados nas suas versões mais atuais, podem servir como uma "brecha" para qualquer invasor.

3.5.2 – Sistema Operacional Windows NT

O Sistema Operacional Windows NT é o sistema mais utilizado no mercado corporativo, devido à tendência de centralização de dados, que por sua vez está crescendo muito, principalmente no mercado nacional.

O fato de o Windows NT ser um Sistema Operacional muito utilizado, ele atrai a atenção tanto dos especialistas em segurança, quanto dos "hackers", com isto surgem diversas "brechas de segurança". Porém, se o sistema for adequadamente configurado, ele se mostrará um sistema altamente seguro.

3.5.2.1 – *Arquitetura de Segurança*

A arquitetura de segurança do Sistema Operacional Windows NT é baseada em diversas atividade e ferramentas que podemos observar, conforme descrito abaixo:

- **Processos de Logon –** estes processos aceitam as solicitações de conexões dos usuários (logon). Neles se incluem os "logon imperativo" inicial que exibe a caixa de diálogo do "logon inicial" para o usuário, e o processo de "logon remoto" que permite o acesso ao sistema por usuários remotos.

➢ **Local Security Authority (LSA) –** este processo garante que o usuário tenha permissão para acessar o sistema. Este componente é o centro do sistema de segurança do Windows NT. Ele gera fichas de acessos, gerencia a política de segurança local e fornece os serviços interativos de autenticação dos usuários. O **LSA** também controla a política de auditoria e registra as mensagens de auditoria, geradas pelo "**Security Reference Monitor".**

➢ **Security Reference Monitor (SEM) –** este processo é o que verifica se o usuário tem permissão para acessar um determinado objeto e executar qualquer ação que esteja tentando. Este componente impõe a validação de acesso e a política de geração de auditoria definida pelo **LSA**. Ele fornece serviços para os modos *Núcleo e Usuário*, para garantir que os usuários e os processos que estão tentando o acesso a um objeto tenham as permissões necessárias. Este componente gera, ainda, mensagens de auditoria quando apropriado.

➢ **Security Account Manager (SAM) –** também conhecido como banco de dados do diretório (directory database) que mantém o banco de dados das contas dos usuários. Esse banco de dados contém as informações para todas as contas de usuários e para as contas dos grupos de usuários. O **SAM** fornece serviços de validação do usuário que são usados pelo **LSA.**

Juntos, esses quatro componentes são conhecidos como Sub-sistemas de Segurança, também chamados de Sub-sistema Integral e não de Sub-sistema Ambiental, porque ele afeta a todo o Sistema Operacional Windows NT.

O modelo de segurança do Windows NT foi projetado para o nível de segurança C2, conforme foi determinado pelo Departamento de Defesa do Estados Unidos da América. Algumas das exigências mais importantes deste nível são:

➢ O proprietário de um recurso (tal como um arquivo) deve ser capaz de controlar o acesso a esse recurso;

➢ O Sistema Operacional deve proteger os objetos para que eles não sejam reutilizados aleatoriamente por outros processos.

Por exemplo, o sistema protege a memória para que seu conteúdo não possa ser lido, depois que ela é liberada por um processo qualquer. Quando um arquivo é excluído, os usuários não poderão ser capazes de acessarem os dados destes arquivos.

Cada usuário deverá ser identificado digitando um nome e uma senha de "logon" única, antes de lhe ser permitido o acesso ao sistema. O sistema deve ser capaz de usar esta identificação única para acompanhar as atividades do usuário.

Os administradores do sistema devem ser capazes de fazerem auditoria nos eventos relacionados a segurança. O acesso aos dados de auditoria deve ser limitado aos administradores autorizados.

O sistema deve se proteger de interferências ou intromissões externas, tais como: modificação no sistema de execução ou alterações nos arquivos de sistemas armazenados no disco.

3.5.2.2 – *Segurança em Ambiente Operacional Misto*

O Windows NT Server tem uma arquitetura de rede aberta que permite flexibilidade na comunicação com outros produtos de rede. Os computadores clientes executando sistemas operacionais diferentes do Windows NT Workstation, ou Windows NT Server podem interagir com computadores em um domínio do Windows NT Server. Entretanto, eles não têm as contas dos computadores do domínio e, portanto, não tem contas de "logon" do Windows NT Workstation.

Os usuários que executam outros sistemas operacionais podem ter as suas contas de usuários armazenadas no banco de dados do diretório, mas o computador em si não tem segurança de "logon" para restringir o acesso aos seus próprios recursos.

Os computadores executando o Windows NT Workstation ou Windows NT Server podem também interagir com servidores e clientes outros sistemas operacionais. Vários protocolos e outros softwares que permitem interoperabilidade estão incluídos no Windows NT Server ou estão disponíveis separadamente.

3.5.2.3 – *Service Pack*

No Windows NT as atualizações são conhecidas como Service Pack (SP) e contém correções de erros, melhoramentos e novas características do sistema. Os SP são acumulativos, por exemplo, o SP3 incorpora todas as alterações do SP 1 e SP 2. A instalação do SP mais recente é um requisito de segurança obrigatório para uma boa política de segurança em rede. O último SP é o de número seis (SP 6).

A Microsoft lançou em 1985 o seu primeiro software de rede chamado PC – LAN, que permitia aos usuários do MS –DOS o compartilhamento de diretórios e impressoras através de uma rede local. A segurança era precária, pois, contava somente com uma senha única em que podia ser colocada em cada compartilhamento. Era mais adequada para o ambiente de microcomputadores, como na época eram chamadas essas plataformas, mas ainda bem distante do que era oferecido pelos Sistemas Operacionais mais avançados, tais como o VMS e o UNIX.

Como o seu funcionamento era considerado razoável, mas tinha uma deficiência no oferecimento de recursos, o Microsoft resolveu aplicar maiores investimentos no desenvolvimento de produtos que pudessem modernizar e oferecer melhores opções aos usuários dos produtos daquela empresa. A cada novo produto lançado no mercado, foram adicionados mais recursos, tornando o que era um protocolo extremamente simples, em um conjunto de rotinas bastante complexas. Ao conjunto de compartilhamento de recursos formados pela: Autenticação dos Usuários, "browsing" e resolução de nomes, chamamos de "***Rede Microsoft".***

3.5.2.4 - *Autenticação no Windows NT*

No ambiente do Windows NT, quando um usuário se "loga", significa que ele foi identificado pelo sistema, sendo assim, ele poderá ter acesso aos recursos da máquina a que ele se "logou".

Entendemos por "Logins" o fornecimento de um nome de usuário e uma senha específica deste usuário que pretende utilizar esse ambiente computacional. Após isso, essa informação e comparada com os registros dos usuários locais e, se estiverem corretas essas informações, o usuário é autenticado "logado".

Os tipos de "login" são:

➢ **Login Local –** quando o usuário está utilizando o ambiente que contém o Windows NT, fazendo um "login" direto, digitando Ctrl + Alt + Del e informando sus conta e a sua senha.

➢ **Login pela Rede –** quando o usuário informa os seus dados, utilizando-se de uma estação de trabalho, e é autenticado pelo Servidor de Rede.

➢ **Login como Serviço –** quando o serviço se identifica para execução com as permissões de um determinado usuário.

Após o "login", os usuários são associados a uma série de privilégios determinando a utilização ou não dos diversos serviços do sistema. Esses privilégios estão contidos em um "token" (barra) que o usuário recebe logo assim que se "loga". Nos poderemos observar estes privilégios e que os possui, através da ferramenta gerenciadora de usuários – **User Manager.**

Uma boa medida de segurança é atribuirmos ao "login local" apenas os usuários que irão se utilizar mais do controle da rede, como por exemplo: *Administradores; Operadores de Backup; DBAs;* etc., negando o acesso aos demais usuários que irão utilizar apenas das plataformas clientes.

3.5.2.5 – *Implementação de uma Política de Senhas*

Para a implementação de uma boa política de senhas, primeiramente devemos seguir as dicas dadas anteriormente, no início deste capítulo. Através da ferramenta *Gerenciamento de Usuários*, nos podemos definir uma política de senhas a ser utilizada pelo Windows NT, como por exemplo:

➢ Fornecer um período de validade das senhas, obrigando os usuários a trocá-las obrigatoriamente e periodicamente;

➢ Não permitir que o usuário utilize as senhas anteriores, mesmo que o sistema armazene as dez últimas senhas por ele usadas;

➢ Bloquear a conta do usuário após um determinado número de fornecimento de senhas incorretas.

Observação Importante: "Esta opção é altamente importante devida a uma grande falha no processo de auditoria do sistema Windows NT, pois, no caso de um "login" incorreto, ele não registra o endereço onde foi feita a tentativa de "log".

A partir do Service Pack 2 no Windows NT 4.0, nos podemos obrigar aos usuários a utilizarem senhas consideradas fortes, isto é, difíceis de serem quebradas. Este SP 2 vem com um arquivo que obriga a que as senhas tenham pelo menos um caractere com, no mínimo três das quatro categorias abaixo:

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

Para habilitarmos esse arquivo, devemos editar o registro utilizando o *REGEDIT* ou o *REGEDIT 32* e digitamos a chave:

HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\System\CurrentControlSet\Control\LSA

Devemos então criar o valor: ***Notification Packages*** do tipo ***REG_MULTI_SZ***, caso ele ainda não exista e adicione ao seu conteúdo a "string" – ***PASSFILT***.

3.5.2.6 – *Auditoria no Windows NT*

Por exigências dos órgão internacionais de segurança, todas as ações do Sistema Windows NT pode ser registradas e auditadas. Ações tais como: acessos aos arquivos; "login" de usuários; execução de programas e impressão de arquivos, etc. são registradas em diretórios do sistema e possibilitam a posterior auditoria, sendo de fundamental importância para os administradores, na verificação de problemas e defeitos, bem como possibilitam a coordenação e a manutenção da integridade e a conseqüente segurança do sistema.

Os registros gerados pela auditoria são acessados pelo "*Visualizador de Eventos*" e são divididos no seguintes tipo diferentes: *sistema, segurança e aplicativos*.

Após a instalação do Windows NT, devemos habilitar a opção de auditoria por segurança que vem, por padrão, desativado. Na janela de configuração de política de auditoria, podemos registrar as seguintes ações:

- **Logon e Logoff –** esta opção permite registrar o sucesso ou a falha na autenticação de um usuário durante o "login", registrando, ainda, a saída de um usuário do sistema. Depois de ativada, esta opção permite saber quais os usuários estavam usando o sistema em um determinado período de tempo e se alguém está tentando usar indevidamente a senha de um outro usuário.

- **Acesso a Objetos e Arquivos –** esta opção permite registrar o acesso, ou as tentativas de acessos, aos arquivos e/ou aos outros objetos do sistema, tais como: compartilhamentos, pipes, registry, etc.

- **Uso dos Direitos dos Usuários –** esta opção permite que, ao ser acionado o sistema, o usuário possa fazer uso dos direitos de acessos e dos privilégios que possua, realizando as tarefas inerentes a esses direitos, tais como: mudar a data e a hora do sistema; acrescentar um componente de domínio, tomar posse de arquivos e de diretórios; etc.

- **Administração de Usuários e Grupos de Usuários –** esta opção permite ao administrador efetuar qualquer tipo de modificação na base dos usuários do sistema, tais como: inclusão ou deleção de usuários; alteração de senhas; etc.

- **Alteração na Política de Segurança –** esta opção permite ao administrador efetuar alterações dos privilégios dos usuários, ou na política de auditoria do sistema.

- **Reiniciar ou Desligar o Sistema –** esta opção, quando implementada, permite que o administrador ou o auditor registrar os processos de "shutdown" (reinicialização) da máquina, bem como a avaliação se os espaços destinados aos arquivos de "log" estão cheios.

- **Controle de Processo –** esta opção é sem dúvidas a mais importante para a implementação de uma política de segurança bem estruturada. Ela permite que o administrador tenha acesso a informações e controle dos processos realizados pelos diferentes tipos de usuários, tendo

como suporte o Windows NT**,** tais como: *início e término das operações dos usuários; objetos acessados; alterações nas bases de dados; ferramentas utilizadas; etc.*

3.5.2.7 – *Principais Vulnerabilidades do Windows NT/2000*

O problema principal para os administradores de redes é não permitir que um intruso consiga atingir os privilégios dos super usuários que, no caso do Windows NT, são os administradores. Por isso, a maior parte das vulnerabilidades descobertas são aquelas que têm por objetivo o status dos super usuários. Assim, qualquer intruso teria como realizar qualquer ação no ambiente computacional.

Analisaremos, agora, algumas das vulnerabilidades que ameaçam a segurança de um sistema que utilize o Windows NT/2000 como suporte.

- **Ataque de Número de Seqüência**

Esta falha ("brecha") está presente em todas as versões do Windows NT e chega a ser de uma classe de grave a crítica, até pelo fato de não existir, ainda, uma solução para esta falha. Consiste no fato da possibilidade da descoberta de uma seqüência de portas abertas no protocolo T, através de um programa de "*caber de portas"*, o que dará ao possível invasor um tipo de permissão completa de acesso que permitirá explorar todo o sistema de arquivos existentes na plataforma.

- **A "Brecha" do RDISK**

O RDISK é um utilitário do sistema Windows NT que permite a criação de discos de reparos de emergência. Para o administrador do sistema esta ferramenta é muito importante, mas ela é uma enorme "brecha" de segurança, pois ela faz um "dump" (levantamento) de todas as informações de segurança existentes no diretório: **C:\WINNT\REPAIR.** Assim sendo, caso o atacante conseguir "crackear" a senha do sistema, em poucos minutos a segurança de uma rede estará 100% comprometida.

A solução para esta falha é simples, bastando adotar a rotina de, após a criação do disco de reparo (RDISK), o administrador do sistema deverá deletar o diretório acima citado.

3.5.3 – <u>Windows 95/98</u>

O fato mais importante que um administrador de redes ou o usuário final precisa saber sobre o Sistema Windows 95/98 é que este sistema não foi projetado para ser um sistema operacional com níveis de segurança altos, como o Sistema Operacional Windows NT, visto anteriormente.

Isto é um risco de conseqüências desastrosas para os administradores e usuários que utilizam este sistema e que não se preocupam com os aspectos de segurança computacional. Este sistema é extremamente fácil de configurarmos, mas também são pequenas as chances de que as pessoas que, mais provavelmente, o configurem tomarem as precauções adequadas, tal como a adoção de uma boa senha.

Além disso, aquele usuário final imprudente poderá estar fornecendo uma "porta dos fundos" para o acesso indevido a sua rede local corporativa, ou armazenando informações sensíveis em um computador doméstico conectado à Internet.

O aumento considerável de conexões com a Internet, por intermédio de cabos ou via DSL de alta velocidade, sempre ativas, este problema somente tende a piorar.

Felizmente, a simplicidade do sistema Windows 95/98 também trabalha a nosso favor, em termos de segurança. Como ele não foi projetado para ser um verdadeiro Sistema Operacional Multiusuário, ele possui recursos de administração remota extremamente limitada. É impossível executar comandos, remotamente, valendo-se deste sistema e utilizando-se de suas ferramentas. Assim, somente é possível o acesso remoto a um registro no Windows 95/98 se este acesso passar anteriormente por um provedor de segurança, tal como o servidor do Windows NT, ou NOVEL NetWare.

Este procedimento é chamado de *Segurança em Nível de Usuário*, versus *Segurança em Nível de Compartilhamento*, baseadas em nome de usuários e senhas e armazenadas localmente. O comportamento padrão do Windows 95/98 não permite que ele haja como servidor de autenticação em nível de usuário.

Assim, existem somente duas maneiras pelas quais os atacantes poderão invadir o sistema Windows 95/98:

- Induzir o operador a executar determinado código;
- Ganhar acesso físico a uma plataforma do sistema, o que será classificado, de acordo com a abordagem em: remota e local.

3.5.3.1 – *Explorações Remotas do Windows 95/98*

As técnicas de exploração remota no Windows 95/98 se enquadram em quatro categorias básicas:

- Conexão direta a um recurso compartilhado, inclusive a recursos discados, ou dial-up;
- Instalação de "deamons" de servidores de portas dos fundos;
- Exploração de vulnerabilidades conhecidas de servidores de aplicativos; e
- Recusa de serviços.

É importante notar que três dessas situações exigem alguma falha de configuração, ou falha de julgamento, por parte do administrador ou usuário do sistema Windows 95/98. Como são falhas de configuração são facilmente remediáveis.

3.5.3.2 – *O Windows 95/98 a partir do Console*

Um usuário precisa se esforçar bastante para tornar um sistema Windows 95/98 vulnerável a comprometimento remoto. Infelizmente, o inverso é verdadeiro, quando um atacante tem acesso físico ao sistema. Na verdade, se houver um tempo suficiente, uma supervisão ruim e um acesso desimpedido à porta dos fundos, o acesso físico normalmente resulta em roubo físico do sistema.

3.5.3.2.1 – *Contramedidas para Hacking de Console*

Uma das soluções tradicionais para a resolução deste problema é configurar uma senha de "BIOS" – Basic Input Output System, codificada fisicamente na placa principal do computador e fornece a função de "*bootstraping"* inicial para computadores PC – compatíveis.

Ela é, desta forma, a primeira entidade a acessar os recursos dos sistemas, sendo que quase todos os fabricantes de BIOS fornecem as funções de bloqueio por senha, as quais podem impedir a ação de intrusos casuais. Atacantes realmente dedicados podem, é claro, remover o disco rígido do computador-alvo e colocá-lo em outra máquina que não seja protegida por senha de BIOS.

Existem, ainda, algumas ferramentas de arrombamento de BIOS disponíveis na Internet, mas as senhas de BIOS normalmente detêm a maioria dos bisbilhoteiros casuais.

Conforme podemos observar pelo exposto acima, o Windows 95/98 é relativamente inerte às ações de atacantes baseados em ambientes de redes, devido a sua falta de recursos internos de "logon" remoto. Praticamente as únicas ameaças reais à integridade de rede Windows 95/98 são o compartilhamento de arquivos que pode ser razoavelmente bem protegido, com uma seleção de senhas apropriadas e pela recusa de serviços que é basicamente resolvida pelo "*Dial-up Networking Update 1.3"*. Todavia, é recomendado veementemente que não se usem como servidores da Internet sistemas Windows 95/98 desprotegidos.

As ferramentas gratuitas "*Back Orifice e NetBus"*, bem como diversas versões comerciais de software de controle remoto, podem compensar de forma bastante razoável a falta de proteção do Windows 95/98 aos "hackers".

Todavia temos a certeza de que se algum intruso tentar obter um acesso físico a um computador cujo sistema operacional é o Windows 95/98, há muito pouco que possa ser feito, o que também é verdade para os outros sistemas operacionais. As únicas proteções que podem garantir um nível um pouco maior de proteção de segurança são as senhas de BIOS e os softwares de proteção feitos por terceiros.

3.5.4 – Novell Netware

Uma idéia incorreta sobre o Sistema Operacional Noell Netware é que os seus produtos são ultrapassados e que, por isso, não têm mais utilidade, como os fabricantes e usuários dos produtos Microsoft e UNIX querem nos fazer acreditar. Embora a participação da Novell não tenha aumentado nos últimos anos, a empresa está muito longe de estar morta e enterrada. Com mais de 40.000.000 (quarenta milhões) de usuários netware no mundo inteiro, o risco de dados corporativos sensíveis nessa rede está mais alto do que nunca. Por mais de 16 anos, servidores Novell abrigaram a maioria dos dados sensíveis e criticamente importantes das organizações.

Para mantermos a integridade dos dados em uma rede local Novell 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 Consócio;**
- **Segurança de Diretório; e**
- **Segurança de Atributos de Arquivos e Diretórios.**

3.5.4.1 – *Segurança de Conexão e Senha*

Para que consigamos desenvolver uma estratégia de segurança de redes, precisamos estar atentos no planejamento, e em todos os detalhes, pois, se não for feita uma boa estratégia de planejamento, certamente ocorrerão problemas, devido a falhas de segurança. Existem dois tipos de segurança de redes:

➢ **Restrições de usuários –** essas restrições limitam o acesso do usuário a certos tipos de funções na rede.

➢ **Restrições de Diretórios de Arquivos –** essa restrições limitam o acesso do usuário a dados específicos.

➢ *Restrições de Usuários*

Primeiro nível de segurança de rede, ele determina que a proteção seja executada por meio de uma senha, e o usuário somente poderá ter acesso à rede, mediante a validação da mesma. Além disso, podemos impedir que um usuário se conecte a 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 de trabalho, ao mesmo tempo, aparecerá uma mensagem de erro, indicativa de que o usuário já está conectado, assim sendo, o acesso à rede lhe será negado.

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

Podemos também, fazer com que o usuário somente possa acessar a rede em um horário pré-estabelecido. Este tipo de restrição, é muito utilizado para fins de manutenção geral, onde podemos eliminar todas as conexões ativas e bloquearmos as conexões, para que a manutenção do sistema possa ser realizada naquele horário.

Observação: "Somente o administrador da rede pode executar esses tipos de restrições de segurança".

➢ *Restrições de Diretórios e Arquivo*

As restrições de diretórios e arquivos, como o próprio nome já diz, limitam os direitos que os usuários têm de acessar os diretórios, ou arquivos específicos, podendo ser atribuídas concessões de acesso diferentes a diferentes sub-diretórios. Para os sub-diretórios que contenham: o sistema operacional, os utilitários e os programas, podemos conceder todos os direitos, a não ser o de procedência e de eliminação, evitando desta forma, a modificação das estruturas dos diretórios, ou remoção de um arquivo de programa.

Outra forma de assegurar a integridade dos dados e das informações é o compartilhamento ("shareable") dos arquivos ou diretórios com características de permissões somente de leitura ("read only).

3.5.4.2 – *Segurança de Consórcio*

Constitui-se no segundo nível de segurança do sistema Novell Netware. Neste nível podemos atribuir privilégios aos usuários e grupos de usuários para trabalharem em diretórios, podendo ser concedido **oito** direitos de consórcio aos usuários, tais como: *leitura, gravação, abertura, criação, eliminação, procedência, pesquisa e modificação* dos arquivos e dos diretórios de dados. Os direitos podem ser concedidos a usuários individualmente ou a todos os usuários de um mesmo grupo.

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

Observação: "Somente o administrador da rede pode atribuir direitos de consórcio aos usuários".

3.5.4.3 – *Segurança de Diretório*

Esse terceiro nível de segurança do sistema Novell Netware, apesar de constar como um nível acima dos níveis anteriormente vistos, ele exerce funções que determinam restrições em um nível abaixo dos níveis anteriores. Assim sendo, ele possui uma precedência sobre o nível de *segurança de direitos de consórcio*, pois, se modificarmos a **máscara de diretórios máximos,** associada a um sub-diretório, poderemos impedir que os usuários da rede exerçam alguns dos seus direitos de consórcio, por estarem cancelados.

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

Exemplo: "Caso o direito de criação se arquivos seja retirado da **máscara de diretórios máximos** do sub-diretório **PROGRAMS**, nenhum usuário poderá criar qualquer arquivo neste mesmo subdiretório, independentemente dos privilégios de consórcios que estes usuários possuam. A **máscara de diretórios máximos** sempre terá precedência sobre os direitos de consórcio. Uma vez que um privilégio tenha sido retirado da **máscara de diretórios máximos**, somente um supervisor de sistema poderá realizar as funções eliminadas".

A combinação dos **direitos de consórcio** com os **direitos de diretório**, determinam o que chamamos de **direitos efetivos dos usuários.**

3.5.4.4 – *Segurança de Atributos de Arquivos e Diretórios*

Quarto nível de segurança do sistema Novell Netware. Os atributos de arquivos e de diretórios têm precedência até mesmo sobre os direitos efetivos dos usuários.

3.5.4.4.1 – *Segurança de Atributos de Arquivos*

Os principais atributos de arquivo e de diretórios são classificados em **partilháveis** (sharable) e não **partilháveis** (non shareable), **leitura e gravação** (read-write) e **somente leitura** (read only) e as suas funções podem ser observadas na tabela abaixo:

ATRIBUTOS	FUNÇÕES
Partilháveis (sharable)	Caso os usuários possuam os direitos efetivos adequados, vários usuários poderão ler o arquivo ao mesmo tempo.
Não partilháveis (non shareable)	Caso os usuários possuam os direitos efetivos adequados, mesmo assim somente um usuários poderá ler o arquivo.
Leitura e gravação (read-write)	Caso um usuário possua os direitos efetivos adequados, ele poderá ler, gravar, eliminar ou trocar o nome de um arquivo.
Somente leitura (read only)	Caso um usuário possua os direitos efetivos adequados, ele somente poderá ler o arquivo.

Quando são criados novos arquivos no sistema Novell Netware são dados a eles atributos do tipo **Não partilháveis** (non shareable) e de **Leitura e gravação** (read-write). Esses atributos permitem que apenas um usuário acesse e manipule o arquivo, considerando que esse usuário tem os direitos efetivos adequados.

3.5.4.4.2 – *Atributos de Diretórios*

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

ATRIBUTO	FUNÇÃO
Escondido ("hidden")	Retira o diretório de vista, durante uma listagem de diretório, mas não impede que os usuários acessem o mesmo.
Privativo (private)	Permite que os usuários vejam o diretório durante uma listagem de diretório, mas não vejam o seu conteúdo.

Importante: *Quando é concedido o direito de consórcio a um usuário em um diretório, ele automaticamente adquire os mesmos direitos em qualquer sub-diretório, a não ser que haja um pedido de restrição.*

3.5.5 – Sistema Operacional UNIX

Durante o ano de 1969, Ken Thompson e, posteriormente, Denis Richie, da AT&T, decidiram que o projeto MULTICS ("Multiplexed Information Computing System" – Sistema de Computação e Informação Multiplexada) não vinha alcançando o desenvolvimento esperado. Decidiram, então, criar um novo Sistema Operacional chamado UNIX e que mudou radicalmente os conceitos de sistemas.

Eles pretendiam que o UNIX fosse um sistema operacional multiusuário robusto e poderoso, e que se sobressaísse no desempenho da execução de programas, em especial programas pequenos chamados de ferramentas. As características de segurança não eram os objetivos principais do UNIX, embora este sistema operacional, efetivamente, tenha um bom desempenho de segurança, quando implementado adequadamente.

3.5.5.1 – *Acesso Remoto*

O acesso remoto envolve um acesso via rede, ou acesso a um outro canal de comunicação, com um modem conectado a um sistema UNIX. Foi descoberto que a segurança de acesso remoto síncrona "RDSI", da maioria das organizações é péssimo.

Às vezes a mídia acaba passando a idéia de que existiria algum tipo de mágica envolvida no comprometimento da segurança do sistema UNIX. Na realidade, existem três métodos para contornar remotamente a segurança do sistema UNIX.

- **Exploração de um Serviço Ouvindo (TCP/UDP)**

Alguém lhe oferece uma identificação e lhe diz, "invada o meu sistema". Este é um exemplo de exploração de um serviço ouvindo. É imperativo lembrar que um serviço precisa estar ouvido para ter acesso, caso contrário, ele poderá ser invadido remotamente.

- **Roteamento por meio de um Sistema UNIX**

Em diversas circunstâncias, atacantes contornam um "firewalls" UNIX, fazendo roteamento de pacotes de fontes por meio do "firewalls" para sistemas internos. Isso é possível quando o encaminhamento IP está ativo no Kernel do UNIX, realizando uma função que deve ser executada pelo aplicativo do "firewalls". Na maioria dos casos, um atacante nunca invade um "firewall" em si, mas simplesmente o usa como roteador.

- **Execução Remota Iniciada por Usuário**

O seu sistema UNIX pode não estar seguro, mesmo tendo sido desativados todos os seus serviços. Pode ocorrer de você navegar até um site qualquer e o seu navegador da Web executar um código mal intencionado o conectar de volta ao site nocivo. É preciso pensar muito nas implicações deste seu ato, principalmente se você estiver conectado com privilégios de "root", enquanto navega na Web.

3.5.5.2 – *Acesso Local*

A maioria dos atacantes se esforçará para ganhar acesso remoto por meio de alguma vulnerabilidade conhecida. Quando um atacante consegue um "Shell" de comando interativo, ele passa a ser considerado usuário local do sistema. Embora seja possível ganhar o acesso direto a um "root" por meio de uma vulnerabilidade, normalmente um atacante ganha acesso de usuário antes.

Assim, um atacante precisará escalar de privilégio de usuário para acesso "root", algo conhecido como "*escalação de privilégio"*. O grau de dificuldade da escalação de privilégio varia muito, dependendo do sistema operacional e também da configuração específica do sistema.

Alguns Sistemas Operacionais fazem um trabalho excelente para impedir que um usuário sem privilégio "root" escale o seu acesso "root", ao passo que outros sistemas são muito fracos neste ponto. Uma instalação padrão do OpenBSD dificultará muito mais que um usuário escale seus privilégios, do que um sistema rodando IRIX. É claro que a configuração individual possui um impacto significativo na segurança geral do sistema.

3.6 – SENHAS

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

3.6.1 – <u>O Quê Não Fazer</u>

Alguns procedimentos de escolha de senhas devem ser evitados, pois, serão facilmente identificadas e quebradas. Alguns sites na Internet fornecem relações de nomes mais usuais encontrados em senhas. Assim sendo, devemos evitar principalmente os seguintes procedimentos:

- Não utilizar nomes de pessoas ou de pessoas da família;
- Não usar números, ou letras repetidas;
- Não utilizar números de documentos (RG, CPF...);
- Não utilizar datas comemorativas (aniversários, casamentos, ...);
- Não repetir o nome de login, ou colocá-lo na forma inversa.

3.6.1 - O Quê Fazer

Para criarmos senhas razoavelmente seguras e que sejam realmente difíceis de serem quebradas, devemos adotar algumas procedimentos, tais como:

- Misturar letras e números e, quando o sistema operacional fizer diferença entre as letras maiúsculas e as minúsculas (Ex.: LINUX), também utilizar.
- Usar símbolos ou caracteres especiais (tabela ASC II), tais como #, %, ^, &, *, etc
- Quando for possível, utilizar ***senhas grandes***, pois, quanto maior for a sua senha, mais difícil de ser quebrada, mas cuidado, ela também se torna difícil de ser lembrada.

Com essas pequenas dicas não podemos garantir que vamos ficar 100% seguros, mas evitaremos pelo menos 80% dos problemas referentes às invasões.

A seguir mostraremos o primeiro evento de violação computacional envolvendo ***Kelvin Mitnick***, o mais famoso dos "crackers".

"Em 1990, ***Kelvin Mitnick*** ficou mundialmente famoso quando invadiu um sistema computacional de uma empresa de cartões de crédito e roubou mais de 20.000 números de cartões de crédito e os distribuiu pela Internet, após o quê, sumiu sem deixar qualquer vestígio".

O FBI levou aproximadamente 5 anos para encontrá-lo e prendê-lo.

Ele foi o primeiro "cracker" a entrar na lista dos dez mais procurados pelo FBI e, depois de quatro anos e meio de prisão, foi colocado em liberdade condicional e, atualmente, trabalha como consultor para assuntos de segurança de uma revista especializada.

A seguir parte da entrevista de ***Kelvin Mitnick.***

Kelvin Mitnick

PRIMEIRA PALESTRA APÓS SER LIBERTADO

Fonte: The Standart - 28 setembro 2002

Depois de quatro anos e meio de prisão e após alguns meses de liberdade condicional, o famoso cracker *Kelvin Mitnick*, deu a sua primeira palestra, durante uma conferência sobre e-Business, promovida pelo Giga Research's Infrastructures. *Kelvin Mitnick* defendeu que o treinamento de funcionários sobre boas práticas de segurança pode ser mais importante do que qualquer tecnologia de ponta. Ele afirmou:

"As pessoas são o elo mais fraco "

Ele citou, ainda, como exemplo "crakers" que muitas vezes enganam alguém de uma empresa, para obter senhas e dados confidenciais, prática essa conhecida como: *engenharia social.*

Preso em 1995, *Kelvin Mitnick* está 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 rádio.

Devemos observar com atenção algumas das recomendações de *Kelvin Mitnick*

- Confirmar a identidade antes de fornecer qualquer informação
- Não escolher senhas óbvias ou que formem palavras
- Não escrever senhas em papéis ou em lugares de fácil acesso
- Trocar de senha freqüentemente
- Usar senhas diferentes para diferentes sistemas
- Usar triturador de papéis para destruir documentos
- Destruir Cds e disquetes, já que dados apagados podem ser recuperados.

Newsletter da Módulo – www.modulo.com.br

CONCLUSÃO

Conforme podemos depreender dos aspectos abordados neste capítulo, chegamos facilmente a conclusão que as características de segurança dos Sistemas Operacionais são de fundamental importância para a garantia da integridade dos nossos ambientes computacionais.

A integração entre os Sistemas Operacionais e os Sistemas Gerenciadores dos Bancos de Dados promovem um nível de segurança adequado, quando bem implementado e corretamente gerenciado. Qualquer desatenção poderá causar danos de valores incalculáveis e que provavelmente não poderão ser resgatados.

A implantação de uma Política de Segurança em uma empresa requer conhecimento dos valores inerentes a esta atividade e o acompanhamento constante da evolução da tecnologia. Todavia, é fator preponderante a participação ativa dos usuários, pois, na realidade, são eles os maiores responsáveis pela operacionalidade dos sistemas. A garantia da integridade dos nossos sistemas é uma responsabilidade pessoal de cada um de nos, não importando o nível em que nos encontramos nas nossas empresas.

A observação nos aponta para uma dura realidade, a maioria dos ataques aplicados nas empresas passam por negligências e não observação das determinações de segurança.

- Nossas senhas são mal escolhidas, fracas e fáceis de serem quebradas;
- Nossos sistemas são gerenciados como se nunca pudessem ocorrer nada de grave contra nos;
- Alguns de nos desconhecem as restrições que os sistemas possuem, ou não estão atentos para as brechas que são periodicamente divulgadas;
- Nossas empresas não investem o suficiente em treinamento de pessoal, principalmente nos conhecimentos dos procedimentos de segurança;

Este e outros aspectos nos deixam preocupados com a situação atual dos níveis de segurança da grande maioria das empresas.

PREVENIR É SEMPRE MAIS FÁCIL E MAIS SIMPLES DO QUE REMEDIAR E, NEM SEMPRE PODEMOS REMEDIAR AS PERDAS OCASIONADAS PELA FALTA DE SEGURANÇA COMPUTACIONAL.

CAPÍTULO IV

SEGURANÇA DAS COMUNICAÇÕES DE DADOS

CAPÍTULO IV
SEGURANÇA DAS COMUNICAÇÕES DE DADOS:

Antes de falarmos sobre segurança na Internet, precisamos entender um pouco sobre o funcionamento das redes de comunicação de dados de um modo geral. Neste capítulo falaremos sobre os protocolos mais utilizados nas transmissões de dados, descrevendo as suas principais características e serviços oferecidos, e como torná-los mais seguro.

Logo no início, os ambientes de processamento de dados que se valiam das redes de comunicação de dados, eram dedicados e cada um fabricante buscava desenvolver seu protocolo, valendo-se das suas arquiteturas proprietárias, configurando redes proprietárias homogêneas.

Assim, as comunicações entre um ou mais equipamentos, eram feitas no modo serial assíncrono. Mais tarde, com a evolução das técnicas de comunicações, e com as transmissões seriais síncronas, esses mesmos fabricantes buscaram adaptar seus protocolos às novas técnicas de comunicação e novos protocolos foram desenvolvidos.

O inevitável desenvolvimento da tecnologia da informação, aliada à necessidade cada vez maior de mantermos nossas comunicações, não só internamente nas redes internas das empresas, mas também com os nossos cliente e fornecedores, forçou o estabelecimento dos protocolos abertos que possibilitassem a conectividade e interoperabilidade entre diferentes plataformas formando as redes abetas heterogêneas.

O estabelecimento do modelo de referência OSI é, na verdade, um marco na era das redes heterogêneas, mas ele não é o único. A ARPANET, como origem histórica da Internet foi o fator determinante para o desenvolvimento do protocolo mais utilizado, no momento, por todos os usuários da grande rede mundial – o TCP/IP.

Assim sendo, estaremos analisando neste capítulo os diversos tipos de protocolos e os seus principais serviços e falhas no aspecto segurança.

4.1 – A REDE MUNDIAL - Internet

As redes de computadores que hoje em dia são utilizadas por milhões de pessoas em todo o mundo quer seja no trabalho ou mesmo em casa, foram criadas a mais de trinta anos. Todavia, a ARPANET – “Advance Research Projects Agency Network” foi desenvolvida nos Estados Unidos da América do Norte, com a finalidade de conectar centros militares de pesquisa. Ela era utilizada por cientistas, para terem acessos a computadores remotos, compartilhar arquivos e enviar mensagens eletrônicas.

A ARPANET deixou de existir em 1990 e a INTERNET, que ocupou mundialmente o seu lugar, continua crescendo de forma assustadora no mundo inteiro. Hoje em dia, ela engloba cerca de 10.000 (dez mil) redes espalhadas em 145 (cento e quarenta e cinco) países, nos cinco continentes. Nesta visão moderna da comunicação mundial, as informações disponíveis na INTERNET ultrapassam os limites físicos, políticos e econômicos dos países e alcançam projeção e crescimento assustador. Assim sendo, garantir a segurança dessas informações é de suma importância para o contínuo desenvolvimento da rede mundial, mas transformou-se em um árduo desafio.

4.1.1 – O Funcionamento da Internet

Para a criação de uma rede de comunicação de dados é preciso que dois ou mais computadores possam ser interligados ao mesmo tempo. Cada um desses computadores formará o que chamamos de "nós da rede", necessita de um conjunto de equipamentos de comunicação para a sua operacionalização.

A INTERNET, neste caso, seria como a "rede das redes", pois ela é a responsável pela interligação de vários redes, de diversos tipos, tais como: *LANs – Local Area Network* (redes locais); *MANs – Metropolitan Area Network* (redes estaduais); e as *WANs – Wide Area Network* (redes nacionais) que conectam computadores no mundo todo e de diversas formas, desde uma simples linha telefônica, até complexas malhas de fibras óticas.

A possibilidade da conexão de dois ou mais computadores, além de dependerem de um conjunto de equipamentos que possibilitem as comunicações, necessita, também, de um software que possibilite essa ligação. Este software, idealizado e construído segundo critérios pré-estabelecidos, é chamado de "***protocolo***" e contém todas as regras e/ou convenções que irão administrar essas comunicações.

Dentre essas regras e critérios estabelecidos para um protocolo estão os níveis de segurança que cada tipo de protocolo deverá atender. Um sistema 100% seguro ainda está muito longe de existir, porém, o nível de segurança que devemos procurar para as nossas empresas deve se aproximar deste nível.

A grande dificuldade encontrada está no fato de que, na mesma proporção, ou até mesmo com maior intensidade com que buscamos assegurar as nossas comunicações e os nossos dados, existem pessoas buscando burlar, quebrar esta segurança.

Resta-nos somente trabalharmos dioturnamente na busca das soluções possíveis e anteciparmo-nos dos inescrupulosos, na tentativa de salvaguardamos nossas empresas.

Esta nossa luta é tão antiga quanto a luta entre o bem e o mal; o construir e o destruir.

4.2 – ANÁLISE DOS PRINCIPAIS TIPOS DE PROTOCOLOS

Passaremos, a seguir, analisar os diversos tipos de protocolos existentes, fazendo uma análise de suas características de segurança e dos seus principais defeitos e "bugs".

4.2.1 - O Modelo OSI DA ISO

A **ISO** (International Organization for Standardization) é uma organização internacional que tem por objetivo a elaboração de padrões internacionais. Os membros da ISO são os órgãos de padronização nacionais dos 89 países membros. O representante do Brasil na ISO é a ABNT.

A ISO é organizada em Comitês Técnicos (Technical Committees – TCs) que tratam de assuntos específicos. Os TCs possuem sub-comitês (SCs) que por sua vez são divididos em grupos de trabalho (Working Groups – WGs).

O desenvolvimento de um padrão ISO começa quando alguma das organizações nacionais acha necessário elaborar um padrão e submete à ISO uma proposta inicial, denominada WD (Working Document). É então formado um WG que trabalha gerando um DP (Draft Proposal). O DP é divulgado e os membros e os membros da ISO têm seis meses para analisá-lo e votá-lo. Se a maioria dos votantes for favorável, um documento revisado chamado DIS (Draft International Standart) é produzido e divulgado. Um novo período de seis meses é definido para a análise e votação. Se o documento for aprovado ele se torna finalmente um IS (International Standart).

O documento da ISO [ISO84, ISO 92], determinou um padrão internacional, denominado Open Systems Interconnection-Reference Model (RM-OSI), e fornecer uma base comum que permite o desenvolvimento coordenado de padrões para interconexão de sistemas. A denominação Open Systems Interconnection (OSI) qualifica padrões para o intercâmbio de informações entre os sistemas abertos (heterogêneos) de comunicação de dados tendo ainda como finalidade do RM-OSI identificar áreas para a elaboração ou aperfeiçoamento de padrões.

Devemos ainda ressaltar que o RM-OSI, por si só, não define a arquitetura de uma rede. Isso acontece porque ele não especifica, com exatidão, os serviços e protocolos de cada camada. Ele simplesmente "diz o que cada camada deverá fazer".

O fato de dois sistemas distintos seguirem o RM-OSI, não garantem que eles possam trocar informações entre si, pois o modelo permite que sejam usadas diferentes opções de serviços / protocolos para todas as camadas do modelo.

A arquitetura OSI estabelece, em conjunto com o esquema básico definido no modelo de referência, orientações e restrições para aperfeiçoar os padrões existentes e guiar o desenvolvimento de novos padrões, visando permitir comunicações seguras e prover uma abordagem consiste para segurança em ambiente OSI.

Essa arquitetura trata exclusivamente dos aspectos de segurança relacionados à comunicação entre os sistemas finais (end systems), não abrangendo medidas de segurança que devam ser adotadas nos sistemas finais, instalações e organizações, para garantir proteção completa dos recursos do sistema, a menos que as medidas tenham implicações nos aspectos de segurança da comunicação.

4.2.1.1 - *Objetivos da Arquitetura de Segurança do Modelo OSI*

Esta seção apresenta os serviços de segurança OSI básicos. Na prática esses serviços são empregados nas camadas em combinação apropriadas, usualmente junto com serviços e mecanismos que estão fora do escopo OSI, para satisfazer os requisitos de uma política de segurança.

A arquitetura de segurança apresentada no documento ISO 7498 – 2 tem os seguintes objetivos:

- Descrever os serviços de segurança OSI e os mecanismos de segurança a eles relacionados.

- Definir a posição dos serviços de segurança e dos mecanismos a eles associados no RM-OSI. Isto é, a(s) camada(s) onde eles devem ser fornecidos.

4.2.1.2 - *Autenticação*

Esse serviço trata da autenticação de entidades que são parceiras em uma comunicação ou da autenticação da entidade que originou uma unidade de dados. O nível de segurança do modele de referência OSI prevê os seguintes tipos de autenticação:

- **Autenticação de Parceiro -** Esse serviço é fornecido para ser usado no estabelecimento de uma conexão, ou esporadicamente durante a fase de transferência de dados de uma conexão, para reconfirmar as identidades das entidades participantes da conexão. O objetivo do serviço de autenticação é garantir que, no momento em que ele é utilizado, uma entidade não está se passando por outra, ou repetindo de forma não autorizada uma mensagem previamente transmitida. Isto é, esse serviço evita ataque dos tipos personificação e replay.

- **Autenticação da Origem de uma Unidade de Dados -** Esse serviço tem como único objetivo autenticar a fonte de uma unidade de dados, não fornecendo proteção contra duplicação ou modificação das unidades de dados.

4.2.1.3 - *Controle de Acesso*

O serviço de controle de acesso fornece proteção contra o uso não autorizado dos recursos, cujo acesso se dê via sistema de comunicação de dados OSI. O requisito necessário para o fornecimento do serviço é o acesso ser viabilizado por protocolos OSI. O serviço de proteção aplica-se a diferentes tipos de acessos a um recurso. Por exemplo: o uso de um recurso de comunicação, a escrita, leitura, ou remoção de informações, ou a execução de recursos de processamento.

4.2.1.4 - *Confidencialidade de Dados*

O serviço confidencialidade fornece proteção aos dados intercambiados no ambiente OSI contra revelação não autorizada da informação neles transportada.

4.2.1.5 - *Integridade de Dados*

O serviço de integridade de dados atua no sentido de proteger os dados intercambiados no ambiente OSI contra ataques ativos que implicam na modificação, remoção ou injeção não autorizada de unidade de dados. Detecta qualquer modificação, inserção, remoção ou retransmissão (replay) não autorizada nas unidades de dados.

4.2.1.6 - *Impedimento de Rejeição*

O serviço de impedimento de rejeição atua impedindo rejeição de serviços, através da prova da identidade das entidades que solicitam a execução de serviços, ou da prova que uma entidade de destino recebeu corretamente uma solicitação para realização de um determinado serviço.

Quando atua provando a origem de uma unidade de dados para o usuário que recebe o pedido de serviço, esse serviço protege a entidade receptora contra qualquer tentativa da entidade transmissora de negar o envio da unidade de dados, ou de seu conteúdo. Por exemplo: um usuário, tendo se arrependido de uma compra realizada através da rede, pode tentar alegar que não foi ele quem enviou a mensagem com o pedido de compra.

A outra forma de utilização do serviço de impedimento de rejeição fornece ao usuário transmissor uma prova de que a unidade de dados por ele transmitida foi corretamente recebida pelo destinatário. Neste caso, o objetivo é proteger o transmissor contra alegações falsas do receptor de que não recebeu a unidade de dados ou seu conteúdo. Aqui, o serviço poderia ser usado, por exemplo, para proteger um cliente de uma companhia aérea que fez a reserva e, ao chegar ao aeroporto para embarcar, é informado de que sua reserva não foi realizada.

4.2.1.7 – *Relacionamento dos Serviços com os Mecanismos de Segurança OSI*

A tabela a seguir apresenta os mecanismos de segurança que, isoladamente ou combinados com outros, são considerados apropriados para o fornecimento dos serviços de segurança OSI. A tabela apresenta uma proposta para o relacionamento entre serviços e mecanismos que, portanto, não representa uma solução única e definitiva para o problema em questão.

Serviços	Mecanismos							
	Criptografia	Assinatura Digital	Controle de Acesso	Integridade de Dados	Intercâmbio de Autenticação	Mascaramento de Tráfego	Controle de Roteamento	Compromisso de Terceiro
Autenticação de Parceiro	SIM	SIM			SIM			
Autenticação da Origem	SIM	SIM						
Controle de Acesso			SIM					
Confidencialidade com conexão	SIM						SIM	
Confidencialidade sem conexão	SIM						SIM	
Confidencialidade em Campos Selecionados	SIM							
Confidencialidade do Fluxo de Tráfego	SIM					SIM	SIM	
Integridade com Conexão e com Recuperação	SIM			SIM				
Integridade com Conexão sem Recuperação	SIM			SIM				
Integridade com Conexão com Recuperação em Campos Selecionados	SIM			SIM				
Integridade sem Conexão	SIM	SIM		SIM				
Integridade sem Conexão em Campos Selecionados	SIM	SIM		SIM				
Impedimento de Rejeição da Origem		SIM		SIM				SIM
Impedimento de Rejeição do Destino		SIM		SIM				SIM

Tabela 1: *Relacionamento entre mecanismos e serviços e serviços de segurança OSI.*

4.2.1.8 - *Relacionamento dos Serviços e Mecanismos Segurança com camadas do RM-OSI*

A definição do posicionamento dos serviços e mecanismos de segurança nas camadas do RM-OSI foi feita tomando por base os seguintes princípios:

➢ O número de formas diferentes de realizarmos um determinado serviço deve ser minimizada.

➢ È aceitável construir um sistema seguro, fornecendo serviços de segurança em mais de uma camada.

➢ A funcionalidade requerida para a segurança não deve duplicar desnecessariamente as funções já existentes no RM-OSI.

➢ A violação da independência das camadas deve ser evitada.

➢ Deve-se evitar a confiança no funcionamento correto das entidades.

➢ Quando uma entidade depender de um mecanismos de segurança implementado em uma entidade de uma camada inferior, todas as camadas intermediárias devem ser construídas para impedir violações da segurança.

➢ Quando possível, as funções de segurança adicionadas devem ser definidas para não impedir sua implementação como um módulo auto contido.

Note que a inclusão de serviços de segurança em uma camada "N" qualquer, implica na modificação de sua interface, para que seus usuários possam solicitar o serviço acrescentado. Além disso, a entidade que implementa o serviço da camada "N" deve ser modificada, de modo que sejam acrescentados os mecanismos de segurança necessários, ou para permitir que a entidade "N" solicite a execução do referido serviço de segurança à camada N-1. A próxima tabela mostra as camadas do RM-OSI, onde os serviços de segurança devem ser fornecidos.

Tabela 2: *Posicionamento dos serviços de segurança nas camadas do RM-OSI.*

Serviços	Camadas						
	1	2	3	4	5	6	7
Autenticação de Parceiro			SIM	SIM			SIM
Autenticação da Origem			SIM	SIM			SIM
Controle de Acesso			SIM	SIM			SIM
Confidencialidade com conexão	SIM	SIM	SIM	SIM			SIM
Confidencialidade sem conexão		SIM	SIM	SIM			SIM
Confidencialidade em Campos Selecionados							SIM
Confidencialidade do Fluxo de Tráfego	SIM		SIM				SIM
Integridade com Conexão e com Recuperação			SIM				SIM
Integridade com Conexão sem Recuperação			SIM	SIM			SIM
Integridade com Conexão com Recuperação em Campos Selecionados							SIM
Integridade sem Conexão			SIM	SIM			SIM
Integridade sem Conexão em Campos Selecionados							SIM
Impedimento de Rejeição da Origem							SIM
Impedimento de Rejeição do Destino							SIM

4.2.2 – O Modelo TCP/IP

No final dos anos 60, ainda com o uso da ARPANET, o Departament Of Defense – (DOD), Departamento de Defesa dos Estados Unidos, decidiu criar as bases de um software de comunicações entre computadores que possibilitaria a troca de informações entre plataformas de diferentes

arquiteturas, não importando as distâncias entre eles e, nem tão pouco, os sistemas operacionais que suportassem essas plataformas.

Assim, os pesquisadores desenvolveram o "***Transmit Control Protocol / Internet Protocol" –*** **TCP/IP**, um modelo de protocolo aberto que também deveria atender as comunicações em sistemas abertos e heterogêneos. Do uso militar, inicial, deste protocolo até o uso indiscriminado na rede aberta mundial Internet, foi somente mais um passo.

Surge então um novo conceito de redes integradas, pois, um sistema de comunicação onde a rede como um todo passou a ser dividida em pequenas redes independentes. Assim, se um segmento da rede parasse, somente este segmento seria afetado. Surgiram, então, os roteadores que interligariam uma rede a outra, isolando o tráfego de dados, mas possibilitando a troca deles entre os computadores.

Logo grandes empresas fabricantes de plataformas computacionais, desenvolvedores de sistemas operacionais e de aplicativos, tais como ***IBM, HP, Compac*** se viram obrigados a compatibilizar seus produtos com este protocolo, tornando-o, assim, um padrão de protocolo de comunicação para Internet.

4.2.2.1 – *As Camadas do TCP/IP*

O modelo **TCP/IP** foi planejado e construído em níveis, ou camadas, cada uma delas com serviços perfeitamente definidos, tais como:

- **Interface de Rede**
- **Rede (IP)**
- **Transporte**
- **Aplicação**

As camadas de Rede e de Transporte têm normas perfeitamente definidas, todavia as camadas de Interface de Rede e de Aplicação não possuem normas definidas, devendo a camada de Aplicação utilizar os serviços da camada de Transporte; e a camada de Interface de Rede deve promover a interface dos diversos tipos de redes com o protocolo, promovendo, em conseqüência, a interoperação entre as diversas arquiteturas de redes.

- *Camada de Interface de Rede* – Esta camada tem como função principal promover a interface entre o modelo **TCP/IP** e os diversos tipos de redes: X.25; ATM; Ethernet; Token Ring, etc.

- *Camada de Rede (IP)* – Também conhecida como a camada Internet, essa camada é responsável pelo endereçamento, roteamento dos pacotes, controle de envio e de recepção de dados, etc.

Dentre os protocolos da camada de rede destaca-se o **IP** (Internet Protocol), **ARP, ICMP, RARP** e os protocolos de roteamento **RIP, IGP, OSPF, Hello, EGP e GGP.**

A camada de rede é uma camada não orientada à conexão, portanto se comunica através de datagramas.

- *Camada de Transporte* – A camada de transporte é uma camada fim-a-fim, isto é uma entidade desta camada comunica com a sua entidade-par do host destinatário. Esta camada faz o controle da conversação ente as aplicações interconectadas da rede.

Esta camada utiliza dois protocolos: **TCP** e **UDP**. O primeiro é totalmente orientado à conexão enquanto o outro não, todavia ambos os protocolos podem servir a mais de uma aplicação simultaneamente.

A camada de transporte transmite dados das várias aplicações simultâneas por intermédio de multiplexação, onde várias mensagens são repassadas para a camada rede, precisamente para o protocolo **IP** que se encarregará de empacotá-las e mandar para uma ou mais interfaces de rede. Chegando ao destinatário, o protocolo **IP** repassa para a camada de transporte que demultiplexa para as portas (aplicações) específicas.

➢ *Camada de Aplicação* – Esta camada é constituída pelas diversas aplicações que compõem o modelo **TCP/IP**. Ela não possui um padrão específico para a camada, o padrão passa a ser estabelecido para cada aplicação, isto é, o **FTP** tem o seu próprio protocolo, assim como o **Telnet, SNMP** e outros.

É na camada de aplicação que se estabelece o tratamento das diferenças entre as diversas representações de formatos de dados.

O endereçamento da aplicação é provido através da utilização de portas para a comunicação com a camada de transporte. Para cada aplicação existe uma porta pré-definida.

4.2.2.2 – *Aplicações do TCP/IP*

Muitos programas do **TCP/IP** podem ser acessados pela Internet e, grandes partes deles, são baseados no modelo *cliente-servidor*, pois quando uma solicitação é recebida, inicia-se um processo de servidor que se comunica com a máquina solicitante.

Cada aplicativo recebe, como especificaremos abaixo, um endereço único, chamado de **porta.** O aplicativo está limitado a essa **porta** em particular e ele é carregado quando uma solicitação de conexão é feita a essa porta.

SERVIÇOS / APLICATIVO	P O R T A
TELNET	**Porta TCP 23**
FTP (File Transport Protocol)	**Porta TCP 21**
SMTP (Simple Mail Transfer Protocol)	**Porta TCP 25**
GROPHER	**Porta TCP 70**
Http (Hypertext Transfer Protocol)	**Porta TCP 80**

Para invadir um computador, um "cracker" utiliza as portas que estão em "listem", ou seja, aceitam conexão de um **IP** externo e, depois, saber quais as versões dos aplicativos utilizados, preparando então um ataque a essa máquina.

Vejamos, agora, alguns desses serviços:

➢ **Telnet (Terminal Virtual)** – Este serviço é utilizado para se permitir que um usuário acesso a um sistema remoto através de uma seção de terminal, operando como se estivesse diretamente conectado neste sistema.

➢ **FTP (File Transfer Protocol)** – Este serviço provê os recurso para permitir a transferência, remoção e eliminação de arquivos, além da criação, modificação e exclusão de diretórios. Para a sua utilização, este protocolo estabelece duas conexões: *conexão de dados e conexão de controle.*

Este serviço não implementa níveis de segurança que fica por conta do **TCP/IP,** exceto as requisições de senhas de acesso a determinados arquivos ou servidores **FTP**.

➢ **SMTP (Simple Mail Transfer Protocol) –** É o protocolo de serviços de correio eletrônico da Internet. Ele fornece serviços de envio e recepção de mensagens para o usuário.

O serviço oferecido pelo SMTP é fonte de inúmeras brechas de segurança devido, principalmente, à má configuração deste serviço.

➢ **RPC (Remote Procedure Control) –** Este protocolo foi criado para suportar as aplicações distribuídas, baseadas em modelo cliente / servidor.

➢ **HTTP (Hypertext Transfer Protocol) –** É o protocolo utilizado pela WEB, ele provê os recurso e serviços necessários à transmissão de textos e qualquer outro tipo de arquivo, além de permitir a navegação na WEB, através de hiper-texto.

4.2.2.3 – *O TCP/IP*

O protocolo **IP** não foi desenvolvido para o ambiente atual da Internet. Embora tenha sido projetado para ser tolerante com algumas falhas de hardware, o **IP** não oferece muita resistência contra ataques. Hoje, a utilização da criptografia é a única forma de proteger os pacotes.

A inexistência de um mecanismo de autenticação permite que invasores possam alterar a origem de diversas conexões. Além disso, o **TCP/IP** representa uma terrível ameaça à segurança, porque permite que usuários remotos ("crackers e hackers") acessem arquivos de outras pessoas.

Caso adotemos o **TCP/IP** na rede interna, devemos utilizar os endereços **IP** reservados para as Intranets, tais como:

➢ De **10.0.0.0 até 10.225.225.225** ou de **172.16.0.0 até 172.16.255.255**

Esses endereços não podem ser usados na Internet e, então, os roteadores do "backbone" da Internet não roteiam contendo esses endereços ficando assim restritos a própria rede interna.

Passaremos, agora, a discutir uma visão resumida da ação do protocolo **TCP/IP**:

Uma transferência tem início com um pedido de leitura ou de escrita de um arquivo. Esta transferência implica em um pedido de conexão. Para estes serviços são utilizados os protocolos **Telnet** ou **FTP**.

Caso o servidor reconheça o pedido, a conexão é aberta e o arquivo é dividido em pequenos pacotes de tamanho fixo de 512 bytes e enviado para o usuário que o solicitou. Essa transferência vai ser realizada sempre em pacotes fixos, até que conclua a transferência. Cada pacote transmitido deve ser reconhecido por um serviço chamado "acknowedgment", antes que próximo pacote seja enviado.

Quando ocorre o envio de um pacote de dados menor do que 512 bytes o usuário servidor sinaliza a conclusão de uma transferência.

Se um pacote extraviar na rede e/ou não conseguir ser reconhecido, o receptor indicará um "*time out"* e retransmitirá o seu último recebido e reconhecido. Isso motiva ao usuário transmissor a retransmitir o pacote perdido. Assim sendo, um usuário transmissor deverá armazenar, temporariamente, somente o último pacote transmitido, uma vez que os pacotes anteriores foram recebidos e confirmados os seus recebimentos.

Como podemos notar, quando duas máquinas estabelecem um "link", são consideradas transmissoras e receptoras.

A transmissora transmite os dados e/ou arquivos sob a forma de pacotes e recebe a confirmação do reconhecimento do pacote recém transmitido.

A receptora recebe os dados e/ou arquivos sob a forma de pacotes sucessivos e envia a confirmação do recebimento, ou a solicitação de retransmissão de um pacote perdido.

Muitos erros podem ocorrer pelo término de um "link". Assim, sempre que houver uma interrupção de um "link" um erro é sinalizado e é enviado um pacote de erro. Este pacote não é reconhecido nem retransmitido (um servidor TFTP, ou um usuário pode terminar, enviando, após, uma mensagem de erro), assim, o outro terminal da conexão não poderá recebê-lo. Portanto, os "time out" são usados para detectar esses términos de "link", quando o pacote de erro for perdido.

O protocolo **IP** define os mecanismos de expedição de pacotes conexão, ele 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 pelo qual os dados serão enviados;
- Inclui um conjunto de regras que envolvem a perspectiva da expedição de pacotes não confiáveis. Essas regras indicam como os "hosts ou gateway" poderiam processar os pacotes; como e quando as mensagens de erro podem ser geradas; e as condições em que os pacotes podem ser descartados.

O protocolo **IP** possui os seguintes tópicos e serviços:

- Endereços **IP**
- Formato dos datagramas **IP**
- Roteamento dos datagramas **IP**
- **ICMP** (Internet Control Message Protocol)

O protocolo **TCP** é um protocolo da camada de transporte. Este protocolo é orientado a conexão, o que indica que neste nível serão solucionados todos os problemas de erros que não forem solucionados no nível **IP**, dado que este protocolo é um protocolo sem conexão. Alguns dos problemas que o **TCP** deve tratar são:

- Pacotes perdidos, ou destruídos por erros de transmissão;
- Expedição de pacotes fora ordem, ou duplicados.

O **TCP** especifica o formato dos pacotes de dados e de reconhecimentos que dois computadores que os dois computadores trocam para realizar uma transferência confiável, assim como os procedimento que os computadores usam para assegurar que os dados cheguem corretamente aos seus destinos. Entre estes procedimentos estão:

- Distinguir entre múltiplos destinos uma máquina determinada;
- Fazer a recuperação de erros, tais como: pacotes perdidos, ou duplicados.

O **DNS** (Domain Name System) é um esquema de gerenciamento de nomes, hierárquico e distribuído. Ele define a sintaxe dos nomes, um banco de dados distribuído que associa nomes a atributos (entre eles o endereço **IP**) e um algoritmo distribuído para mapear os nomes e os endereços.

As aplicações normalmente utilizam um endereço **IP** de 32 bits, para abrir uma conexão, ou enviar um datagrama **IP**, todavia, os usuários preferem identificar as máquinas através de nomes ao invés de números. Assim sendo, um banco de dados que permita a uma aplicação encontrar um endereço, a partir do nome com que a máquina é referenciada, é extremamente necessário.

Um conjunto de servidores de nomes mantêm os bancos de dados com os nomes e os endereços das plataformas conectadas a Internet. Na realidade, este é apenas um tipo de informação armazenada no "domain system" (sistema de domínios). Note que é usado um conjunto de servidores interconectados, ao invés um único servidor centralizado.

Existem, atualmente, tantas instituições (servidores) conectados a Internet que seria impraticável exigir que elas notificassem uma autoridade central, toda vez que uma nova plataforma e/ou novo usuário se conectasse, ou mudasse de lugar. Assim, a autoridade delega às instituições a competência da atribuição dos nomes que irão referenciar as plataformas.

Os servidores de nome formam uma enorme árvore, correspondendo a estrutura institucional. Os nomes também adotam uma estrutura similar.

Tomemos por exemplo o nome ***"<nome>.abc.xyz.br"***.

Para encontrarmos o 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 está 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 nomes para o nível "**br**" (podem existir mais de um servidor de nomes em cada nível, para garantir a continuidade da operação quando um deles pára 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**" é possível solicitar que ele informe o endereço do servidor "**abc**". A partir deste ponte pode-se encontrar consultar o servidor "**abc**" sobre o endereço da plataforma **<nome>.** O resultado final da busca é o endereço Internet correspondente ao usuário ***"<nome>.abc.xyz.br"***.

Cada um dos níveis percorridos é referenciado como sendo um domínio. O nome completo ***"<nome>.abc.xyz.br"*** é um nome de domínio. Na maioria dos casos, não é necessário acessar a todos os domínios de um nome para encontrar o endereço correspondente, pois, os servidores de nomes muitas vezes possuem informações sobre mais de um nível de domínio, o que poderá eliminar mais de uma consulta.

Além disso, as aplicações normalmente têm acesso ao **DNS** através de um processo local (o servidor para as aplicações é 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 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 todos as aplicações que fazem uso do **DNS,** o algorítimo de encaminhamento na árvore de domínios descrito anteriormente.

O **DNS** não se limita a manter e gerenciar endereços na Internet. Cada nome de domínio é um nome em um banco de dados que pode conter registros definindo várias propriedades, tais como o tipo da plataforma, a lista de serviços fornecidos por ela, etc.

O **DNS** permite que seja definido um nome alternativo para o número de identificação. Também é possível utilizar o **DNS** para armazenar informações sobre os usuários, listas de distribuição ou outros objetos.

O **DNS** é particularmente importante para o sistema de correio eletrônico, pois nele são definidos os registros que identificam a máquina que manipula as correspondências relativas a um determinado nome, identificando, assim, onde um determinado usuário recebe suas correspondências. Ele pode, ainda, ser utilizado para definição das listas para a distribuição de correspondências **SMTP – Simple Mail Transfer Protocol**.

O **SMTP – Simple Mail Transfer Protocol** é o protocolo usado no sistema de correio eletrônico na arquitetura **TCP/IP.** Este protocolo especifica como o sistema de correio eletrônico transfere mensagens de uma máquina para outra. O módulo de interface com o usuário e a forma como as mensagens são armazenadas não são definidos por este protocolo. O sistema de correio eletrônico pode, também, ser utilizado por processos de aplicação para transmitir mensagens contendo textos.

4.3 - SEGURANÇA NA INTERNET

O termo *arquitetura de segurança* de uma rede pode ser empregado com conotações diferentes, para isso, uma arquitetura de segurança consiste na definição de conceitos e de terminologias que formam um esquema básico para o desenvolvimento de um protocolo. No caso específico da Internet, espera-se que a arquitetura de segurança forneça um conjunto de orientações mais concreta, voltadas também para projetistas de redes e desenvolvedores de produtos, e não apenas para os projetistas de protocolos.

Isso sugere que a arquitetura de segurança da Internet englobe não apenas definições de conceitos , como faz o padrão ISO/OSI, mas inclua adicionalmente orientações mais específicas sobre como e onde implementar os serviços de segurança na pilha do protocolo da Internet. Esta visão alinha-se com a filosofia da Internet que enfatiza a interoperabilidade entre sistemas, produzindo padrões que tendem a ser menos genéricos que os padrões estabelecidos pelo modelo OSI/ISO.

Tudo indica que a segurança da Internet adotará a definição de serviços, mecanismos e ameaças do padrão OSI. Cabe, entretanto, destacar que a adoção da terminologia usada não implica na adoção dos mapeamentos dos serviços nas camadas OSI e dos mecanismos de segurança nos serviços implementados nessa arquitetura.

Além dos princípios de segurança no modelo OSI, serão adicionados os seguinte princípios para a escolha dos mecanismos:

- *Os mecanismos de segurança devem ser escaláveis, tendo capacidade e potencial para acompanhar o crescimento da comunidade Internet;*

- *Os mecanismos devem ter sua segurança apoiada na tecnologias que os suporta, por exemplo, em algorítimos e protocolos que sejam seguros, isto é, que não possuam falhas intrínsecas;*

- *Os mecanismos de segurança não devem restringir a topologia da rede;*

- *Mecanismos de segurança não estejam sujeitos às restrições de controle de exportação ou patentes, devem ter prioridades;*

- *È sabido que muitos mecanismos de segurança necessitam de uma infra-estrutura de apoio, o gerenciamento dessa infra-estrutura pode ser tão ou mais complexo que a implementação do mecanismo. Assim, deve-se dar preferência às tecnologias de segurança que possam compartilhar uma infra-estrutura de segurança comum.*

- *Os algorítimos de criptografia selecionados para padronização na Internet deve ser amplamente conhecidos, devendo ser dada preferência aos que tiverem sido exaustivamente testados.*

4.3.1 – Equipamentos de Redes e os Níveis de Segurança

Um projeto de rede tem, obrigatoriamente, que utilizar alguns equipamento necessários às comunicações. Analisar as suas característica e as possibilidades de garantir níveis de segurança é um fator fundamental de planejamento para que possamos estabelecer nossas comunicações em níveis razoavelmente seguros. Passaremos a analisar os principais equipamentos utilizados e as suas características.

4.3.1.1 – *ROTEADORES* (Routers)

Geralmente, os roteadores são computadores normais que possuem mais de uma interface de rede. Neste caso, o roteamento é executado através de um software, porém, quando o tráfego inter-rede é muito alto, são utilizados equipamentos especificamente desenvolvidos para esta função.

A principal função do Roteador é encaminhar os pacotes de comunicações em uma rede ou entre redes, sendo responsável por saber como toda a rede está conectada e como as informações

podem ser transmitidas de uma parte da rede para outra, evitando-se assim que os "hosts" percam tempo assimilando conhecimento sobre a rede. Para identificar o destino dos pacotes os roteadores utilizam os endereços **IP**. Cada computador tem registrado uma tabela de roteamento **IP**, onde as entradas são pares: *endereços de rede e endereço de roteador*.

A especificação de rotas especiais ou obrigatórias para as transferências de dados, pode nos possibilitar a garantia de que os dados sejam transmitidos em rotas fisicamente seguras, ou para garantir que as informações mais sensíveis sejam transportadas por rotas com canais que contenham níveis de proteção mais apropriados.

Para garantirmos um maior nível de segurança, podemos utilizar os roteadores para manter um isolamento estratégico, permitindo que dois grupos de equipamentos se comuniquem entre si e, ao mesmo tempo, continuem isolados fisicamente.

Utilizando as funções de filtragem dos roteadores, podemos controlar, com vigor, quem utiliza a rede e quais os serviços são utilizados por esses usuários. Por essa função de filtragem, os roteadores são incorporados à política de segurança das redes. A implementação correta e eficiente desses dispositivos coloca-os em um patamar de comparação com um "firewall" (parede de fogo), bloqueando os acessos indesejáveis, para vários tipos de portas e de protocolos.

Um fator importante e que devemos estar atento é a desvantagem criada por essa implementação, são os períodos de lentidão da rede que mesmo imperceptíveis para o usuário comum, deverão ocorrer com freqüência.

O roteamento na Internet é realizado por protocolos como **BGP, EGP** e **OSPF.** Todos esses tipos de protocolos possuem requisitos de segurança semelhantes: *autenticação de parceiros e integridade no intercâmbio de datagramas, carregando informações de roteamento.* Caso seja preciso proteger as informações sobre a topologia da rede, é necessário garantir a confidencialidade dos datagramas.

A maior parte desses serviços pode ser fornecida com a utilização de mecanismos genéricos da camada de rede, ou podem ser construídos especificamente para os protocolos de roteamento. Neste caso, a granularidade da autenticação e do controle de acesso é claramente atingida pelas informações de identificação fornecidas nessa camada. A variedade dos protocolos de roteamento torna óbvio os benefícios de utilizarmos mecanismos de segurança comuns fornecidos na camada de rede.

O serviço de confidencialidade do fluxo de tráfego ponto-a-ponto pode ser fornecido aos usuários pelo roteador, utilizando mecanismos do nível físico. Todavia, para garantir a confidencialidade quando os pacotes trafegam por vários roteadores em seu caminho, é necessário utilizar o serviço de confidencialidade do nível rede.

Os roteadores são equipamentos muito importantes na configuração das redes de teleprocessamento, as suas características de operações e os níveis de segurança que eles oferecem como proteção de integridade das transmissões de dados devem ser observados atentamente quando do planejamento das redes.

4.3.1.2 – ***FIREWALL*** (Parede de Fogo)

Uma das maiores preocupações com segurança na Internet é a vulnerabilidade de um computador, comprometendo a troca de informações pelos meios físicos da rede na qual está ligado. Um dos dispositivos utilizados para aumentar os níveis de segurança das redes ligadas à Internet é o

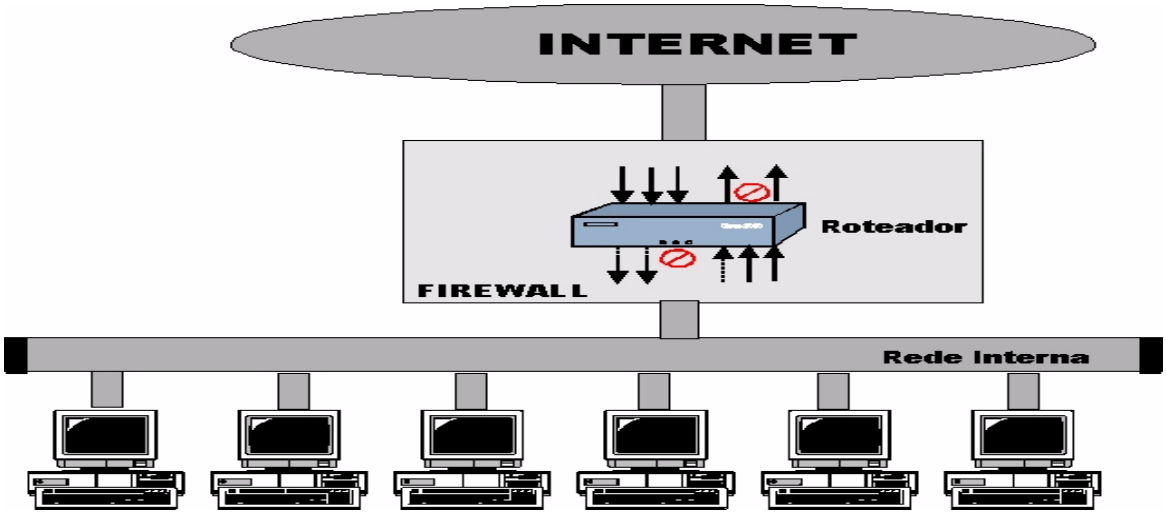
"FIREWALL" que é uma espécie de barreira de proteção, fazendo um bloqueio de qualquer acesso indevido vindo da Internet, para dentro da sua rede local.

O "FIREWALL" geralmente é um computador independente da rede, mas pode ser utilizado também um roteador, ou um dispositivo de hardware proprietário. A sua principal função é fazer uma avaliação de cada solicitação de conexão ao seu computador. Após sua verificação, baseada em uma lista de restrições e permissões, anteriormente configurada conforme as necessidades de segurança para a comunicação da rede interna com a Internet, faz-se a autorização da conexão. A configuração correta de um "FIREWALL" é a chave de sucesso para a segurança de uma rede.

Todos os acessos da sua rede para a Internet devem passar pelo "FIREWALL". Nos temos que ter a certeza de que não há nenhum computador com acesso remoto a Internet via "modem" e que possa ser transformado em uma "porta" de acesso indevido, destruindo, ou melhor, colocando em risco todo o seu esforço em garantir a segurança da nossa rede.

A utilização de barreiras de proteção fundamenta-se no fato de que normalmente a segurança é inversamente proporcional à complexidade dos sistemas. Assim, proteger máquinas de uso geral, onde são executadas diferentes aplicações, de vários portes, é uma tarefa complicada, pois é muito improvável que nenhuma das várias aplicações apresente falhas que possam ser exploradas para violar a segurança do sistema. Assim, fica muito mais fácil garantir a segurança isolando as máquinas de uso geral de acessos externos usando uma barreira de proteção, ou "FIREWALL" que impeçam a exploração das possíveis falhas.

O princípio da simplicidade tem como conseqüência a seguinte consideração: "*para diminuirmos os riscos de violações, a configuração do "FIREWALL" deve ser minimizada, excluindo tudo que não seja estritamente necessário*".



Um "FIREWALL" é definido como um conjunto de componentes, colocados entre duas redes que, coletivamente, possua as seguintes propriedades:

- Todo o tráfego de dentro para fora da rede vice-e-versa, passa pelo "FIREWALL".
- Somente o tráfego autorizado pela política de segurança pode atravessar o "FIREWALL".
- O "FIREWALL" deve ser a prova de violações.

O "FIREWALL" pode ser visto como um monitor de referências para uma rede, sendo o seu objetivo garantir a integridade dos recursos ligados a ela. A centralização demanda uma administração mais cuidadosa por parte dos administradores do sistema, da máquina que implementa o "FIREWALL".

Enquanto as máquinas de uso geral são configuradas para otimizar o desempenho e a facilidade de utilização, no "FIREWALL" tudo isso passa para um segundo plano, cedendo lugar ao seu objetivo principal no sistema: a segurança.

Os filtros (*"screens")* bloqueiam a transmissão de certas classes de tráfego. O componente "*gateway"* é uma máquina, ou um conjunto de máquinas conectadas por um segmento de rede que fornecem serviços de retransmissão.

O filtro colocado na saída da rede entre a rede externa e o "*gateway*", é usado para proteger o "*gateway*" de ataques externos, enquanto que o filtro interno protege a rede interna das conseqüências de um ataque que tenha conseguido comprometer o funcionamento do "*gateway*".

Assim, os dois filtros atuando isoladamente, ou em conjunto, protegem a rede interna de ataques externos. Um "*gateway do firewall*" que pode ser acessado a partir da rede externa é chamado de "*bastion host"*.

Os "Firewalls" são classificados em três categorias principais:

- ***Filtros de Pacotes*** – Utilizam os endereços **IP** de origem e de destino e as portas **UDP** e **TCP** para tomar as decisões de controle de acesso. O Administrador da rede elabora uma lista de máquinas e de serviços que estão autorizados a transmitirem datagramas nos sentidos possíveis de transmissão e que será usada para filtrar ao datagramas dos **IP** que tentam atravessar indevidamente um "*firewall"*.

  Um exemplo de política de filtragem de pacotes seria: permitir o tráfego de datagramas carregando mensagens SMTP e DNS nas duas direções e tráfego de Telnet somente para os pacotes saindo da rede e impedir todos os outros tipos de tráfego de mensagens.

- ***Gateways de Circuitos*** – Este tipo de *firewall* atua como intermediário de conexões **TCP,** funcionando como um **Proxy** (um **TCP** modificado). Para transmitir dados através do *firewall*, o usuário origem conecta-se a uma porta **TCP** no "*gateway*" e este, por sua vez, conecta-se, usando uma outra conexão **TCP**, ao usuário de destino.

  Um circuito é formado por uma conexão **TCP** na rede interna e outra na rede externa, associados pelo "*gateway de circuito*". O processo que implementa esse tipo de "*gateway*" atua repassando bytes de conexão para outra, fechando o circuito.

  Para que seja estabelecido um circuito, um usuário de origem deve fazer uma solicitação ao "*gateway no firewall*", passando como parâmetros a máquina e o serviço de destino. O "*gateway*", então estabelece o circuito ou, caso contrário, retorna um código informando o motivo do não estabelecimento da conexão.

  Devemos notar que o usuário de origem utiliza um protocolo simples, para se comunicar com o "*gateway*". Esse protocolo é um bom local para implementarmos, por exemplo, um mecanismo de autenticação.

- ***Gateway de Aplicação*** – Este tipo de *firewall* utiliza implementações especiais das aplicações desenvolvidas especificamente para funcionarem de forma segura. Devido a grande flexibilidade dessa abordagem, ela é a que pode fornecer o maior nível de segurança.

  Por exemplo, um "*gateway*" **FTP** pode ser programado para restringir as operações de transferências de arquivos fisicamente localizados no "*bastion host"*. Assim, os usuários externos somente podem ter acesso aos arquivos disponibilizados nessa máquina.

Alguns *firewalls* encontrados no mercado têm a opção de tornar nossos sistemas invisíveis ao mundo externo, por exemplo: O Sun Scren da Sun Microsystems, oferece a capacidade não-**IP**, isso é, dificuldade para identificar os nós da rede.

Os *firewall* são muito eficientes nas questões de segurança, mas reservam algumas armadilhas que podem prejudicar a funcionalidades das redes, como por exemplo: em ambientes nos quais os usuários dependem de aplicativos distribuídos, a configuração de um *firewall* passa a ser um pouco complicado, pelo fato deles terem um diretiva de segurança muito restrita, o ambiente acaba se tornando pesado, lento, ocorrendo perdas da funcionalidade da rede.

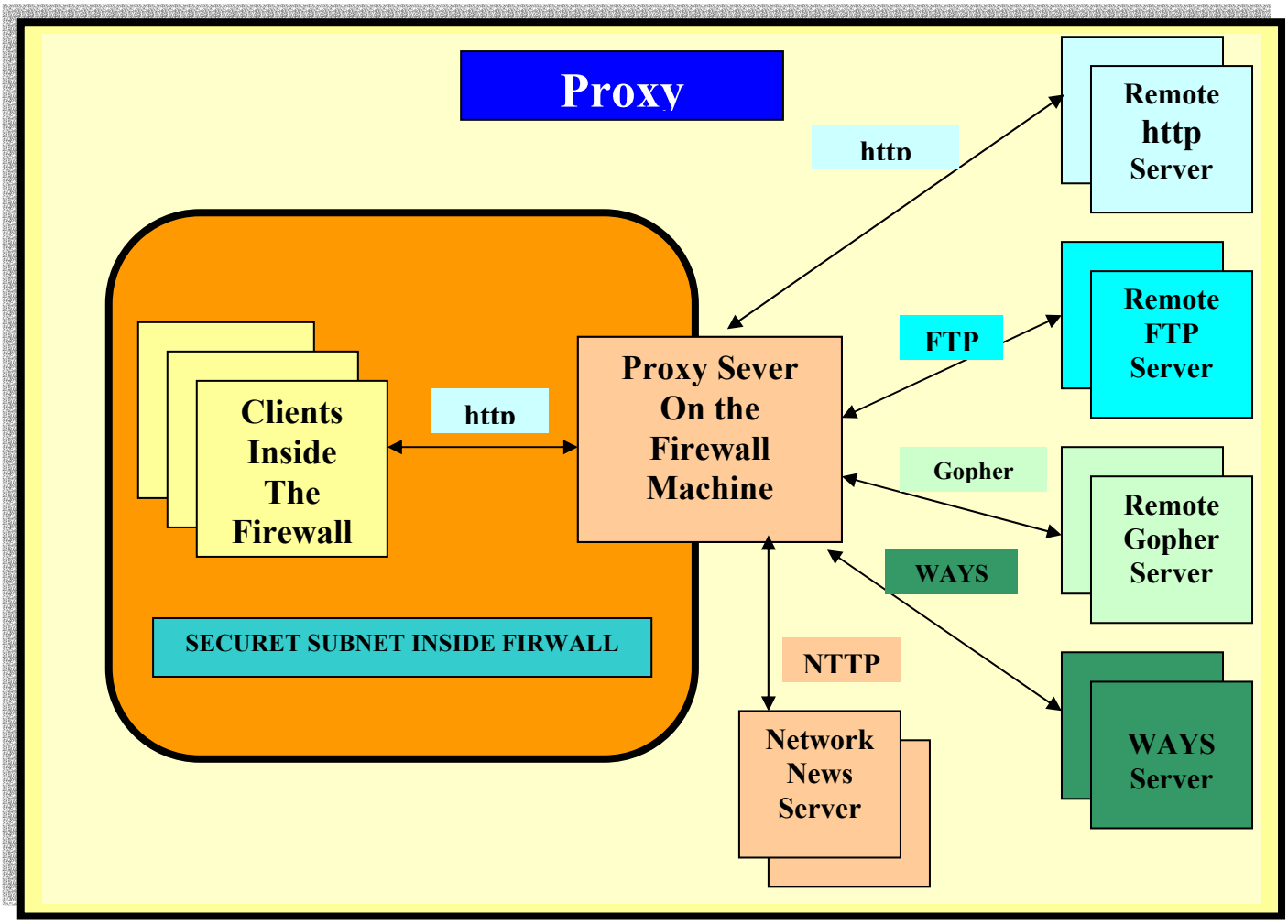
Outro fato importante e que devemos atentar é que o *firewall* coloca toda a sua rede, usando o sentido figurado, "dentro de uma caixa" que se for aberta, comprometerá toda a segurança das informações da empresa. Em outras palavras, seu *firewall* for burlado a sua rede estará totalmente vulnerável, podendo ser completamente destruída. Assim sendo é recomendável que adotemos outras técnicas de segurança além do *firewall*.

Passos importantes na construção de um *firewall*:

- ***Identificar a topologia, o aplicativo e as necessidades de protocolo da rede;***
- ***Analisar os relacionamentos de confiança em sua organização;***
- ***Desenvolver diretivas baseada naquelas necessidades e relacionamentos;***
- ***Identificar o*** *firewall correto para, a configuração específica;*
- ***Empregar esse*** *firewall corretamente;*
- ***Testar as diretivas corretamente.***

4.3.1.3 - ***PROXY***

Outro dispositivo utilizado para aumentar os níveis de segurança das redes ligadas à Internet é ***PROXY*** que nada mais é do que um tipo de *firewall*. Sua atuação vai desde restringir o acesso a alguns sites até fazer o gerenciamento dos pacotes **IP** que vão trafegar na nossa rede.



Uma vantagem do *Proxy* é o "*cache"* que é a capacidade do servidor *"proxy"* de armazenar informações já acessadas na Internet, utilizando-as para solicitações futuras de usuários, evitando um novo acesso á mesma informação.

Um nível de aplicação *Proxy* deixa um *firewall* seguramente permeável para os usuários na organização sem criar brechas na segurança.

O *Proxy* permite um alto nível de "log" das transações de clientes, incluindo **IP**, data e hora e **URL,** etc. Qualquer campo em uma transação **http** é um candidato para log, fato impossível no nível **IP** ou **TCP**.

Também é possível fazermos filtragem de transações de usuários no nível do protocolo de aplicação, este protocolo pode controlar o acesso por métodos individuais, servidores, domínio, etc.

CONCLUSÃO

Está mais do que claro que a Internet, por não ter sido planejada e disponibilizada para operação como uma rede mundial de largos serviços, não é absolutamente segura. Isto posto, como convivermos com um ambiente computacional inseguro e disponibilizarmos recursos e serviços aos nossos usuários e parceiros?

Não que isto seja uma resposta fácil, todavia está perfeitamente claro que, a partir do conhecimento da fragilidade dos serviços disponíveis na rede, podemos agregar recursos e medidas que irão suprir corretamente esta falta.

A escolha adequada de software e hardware específicos de segurança computacional, eleva o nível de segurança e resguarda a empresa de imprevistos cujas conseqüências são lastimáveis. Nada irá suprir as perdas ocasionadas pela não observação das fragilidades, pois elas serão na maioria das vezes irrecuperáveis.

Um Firewall, ou um Proxy bem escolhidos e direcionados para as atividades da empresa, certamente favorecerão a segurança e evitarão grande parte dos nossos transtornos e aborrecimentos, todavia esses equipamentos por si só não são a garantia da total segurança. Uma política bem definida, o uso adequado das senhas, as divisões dos usuários em grupos e a administração dos recursos computacionais de forma adequada são medidas que se complementam e devem ser adotadas.

Finalmente, devemos nos preocupar com os serviços prestados por nossos provedores. A negligência e a falta de conhecimento específico por parte dos profissionais que administram tais recursos é grande e traz sérias conseqüências. Devemos sobre tudo exigir dos nossos provedores um mínimo de atenção para com os serviços que se propõem oferecer.

CAPÍTULO V

CRIPTOGRAFIA E ASSINATURA DIGITAL

CAPÍTULO V
CRIPTOGRAFIA E ASSINATURA DIGITAL

Quantas vezes nos não pensamos em enviar uma mensagem para alguém se que mais ninguém a conseguisse ler? Para fazermos isso é fácil, basta garantir que mais ninguém tenha acesso a esta mensagem. Mas como fazer isso, quando esta mensagem for transmitida por um meio não seguro, como pro exemplo a Internet?

Quando enviamos qualquer informação pela Internet, seja um arquivo ou um simples e-mail, esta informação passa por diversas máquinas, antes de atingir o destinatário. Nesse caso, o único meio de garantir a integridade desta mensagem seria escrevê-la de um modo que somente o destinatário a pudesse entender, ou seja, criptografá-la.

A criptografia, embora tenha origens muito antigas, vem sendo, atualmente, muito utilizada. Em quase todas as operações realizadas na Internet que envolva troca de dados sigilosos, como o envio de uma senha, ou número de cartão de crédito, a criptografia deverá ser utilizada.

Mas, junto com os avanços conseguidos nos métodos de criptografia, os hackers também se sofisticando cada vez mais. UM método de criptografia nunca é totalmente seguro. O que os diferencia é a dificuldade de se "quebrar" a chave.

Quanto mais tempo demorar em se conseguir ler a informação original, mais segura é a criptografia. Esse capítulo tem o objetivo de estudar esses diferentes métodos, e orientar os administradores e gerentes sobre os diversos métodos para se criptografar uma informação, possibilitando que, ao se depararem com a necessidade de optarem por um desses métodos o faça de modo que o método escolhido dificulte ao máximo a ação dos hackers.

Um sistema criptográfico é composto por algorítimos cujas ações são influenciadas por valores conhecidos como ***chaves***. A ação do algorítimo depende tanto dele quanto do valor da chave. O tamanho de uma ***chave*** é medido em bits e a segurança do texto cifrado depende do tamanho da ***chave***, do grau de dificuldade para se descobrir o valor da ***chave*** e do grau de dificuldade para se decifrar os dados sem que se conheça a ***chave***. Em um sistema criptográfico forte, a segurança depende das ***chaves*** serem mantidas em segredo e não do algorítimo de criptografia ser mantido em segredo.

A criptografia moderna possui dois grandes grupos, diferenciados por características especiais que as definem: ***Criptografia de Chave Simétrica e Criptografia de Chave Assimétrica.***

5.1 – CONCEITO GERAL E FUNDAMENTOS DA CRIPTOGRAFIA

A criptografia é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de códigos. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

Criptografia (kriptós = escondido, oculto; grápho = grafia) é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e compreenda, ou seja, criptografia transforma textos originais, chamados texto original (plaintext) ou texto claro (cleartext),

em uma informação transformada, chamada texto cifrado (ciphertext), texto código (codetext) ou simplesmente cifra (cipher), que usualmente tem a aparência de um texto randômico ilegível.

5.1.1 - Termos utilizados

A ciência da criptografia usa termos particulares para a determinação de atividades e a conceitualização de níveis e objetivos. A seguir definiremos alguns desses termos:

- **Criptografia** (kriptós = escondido, oculto; grápho = grafia): é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e a compreenda.

- **Criptoanálise** (kriptós = escondido, oculto; análysis = decomposição): é a arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque.

- **Criptologia** (kriptós = escondido, oculto; logo = estudo, ciência): é a ciência que reúne a criptografia e a criptoanálise.

- **Cifrar** é o ato de transformar dados em alguma forma ilegível. Seu propósito é o de garantir a privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados.

- **Decifrar** é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível. Para cifrarmos ou decifrarmos uma mensagem, necessitamos de informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes.

5.1.2 – Objetivos da Criptografia

A criptografia computacional, como a conhecemos, protege o sistema quanto à ameaça de perda de confiabilidade, integridade ou não repudiação, é utilizada para garantir:

- **Sigilo**: somente os usuários autorizados têm acesso à informação.

- **Integridade**: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

- **Autenticação do usuário**: é o processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que alega ser.

- **Autenticação de remetente**: é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem.

- **Autenticação do destinatário**: consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.

- **Autenticação de atualidade**: consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

O único método disponível para oferecer proteção contra esses tipos de fatos, tanto durante o armazenamento quanto em trânsito é a criptografia.

5.1.3 - O que a Criptografia não Protege

Não adianta imaginarmos que a criptografia irá solucionar todos os nossos problemas de segurança. Existem coisas que, por maior e melhor que sejam os processos de criptografia, não conseguimos proteger. Assim, podemos citar o que a criptografia não protege:

- Criptografia não impede um atacante de apagar todos os seus dados.

- Um atacante pode comprometer seu programa de criptografia. O atacante pode modificar o programa para usar uma chave diferente da que você gerou ou talvez gravar todas chaves de encriptção em um arquivo para análise posterior.

- Um atacante pode encontrar uma forma relativamente fácil de decriptografar as mensagem conforme o algorítimo que você esteja usando.

- Um atacante pode acessar seus arquivos antes de você encriptá-lo ou após a decripatação.

- Por tudo isso, a criptografia deve fazer parte da sua estratégia de segurança, mas não deve ser a substituta de outras técnicas de segurança.

5.2 - TÉCNICAS BÁSICAS DE CRIPTOGRAFIA

Os algorítimos de criptografia efetuam permutações sobre os bits ou os caracteres do texto, de modo a tornar indecifrável o significado do texto resultante, a não ser que seja conhecida uma "password" que permita sua decodificação. Existem duas técnicas básicas para compormos os algorítimos de criptografia:

- **Transposição** - Cifra de transposição (algumas vezes chamada de cifra de permutação) reorganiza a ordem dos bits, caracteres ou bloco de caracteres.

Vejamos um exemplo muito simples de transposição, as letras do texto original (texto plano) são embaralhadas. Com este tipo de cifra, as letra originais do texto plano são preservadas, existe somente uma troca de posições.

NUCLEAR ==>	*ENCRIPTAÇÃO* ==>	LUCNARE

- **Substituição** - Cifra de substituição troca os bits, caracteres ou blocos de caracteres por outros (por exemplo, uma letra é trocada por outra). Um exemplo clássico de substituição é a cifra de César, que substitui as letras avançando três casas dentro do alfabeto.

Agora um exemplo também muito simples de cifra de substituição, as letras do texto plano são trocadas por outras letras, números ou símbolos. Com este tipo de cifra as posições originais das letras do texto plano são preservadas, mas as letras são substituídas por outras.

NUCLEAR ==>	*ENCRIPTAÇÃO ==>* Troca de cada letra do alfabeto pela próxima letra do alfabeto.	**O V D M F B S**

NUCLEAR ==>	*ENCRIPTAÇÃO ==>* Troca de cada letra do alfabeto pelo número de representação da letra dentro do alfabeto.	**14 21 3 12 5 1 18**

5.2.1 – Tipos de Criptografia

Os algorítimos de criptografia podem seguir regras pré-estabelecidas que irão definir o tipo de criptografia realizada. Cada uma dessas regras possui as suas vantagens e desvantagens, mas somente o estudo detalhado da necessidade da empresa é que poderá determinar qual a melhor técnica e a que deveremos adotar. As técnicas são classificadas em:

- **Criptografia de Chave Simétrica**
- **Criptografia de Chave Assimétrica**
- **Assinatura Digital**
- **Criptografia Combinada de Chave Pública e Criptografia de Chave Simétrica**

Os modernos algorítimos de criptografia podem ser classificados em dois tipos de acordo com a chave que utiliza: os de **chave única** e os de **chave pública e privada**.

5.2.1.1 – *Criptografia de Chave Simétrica*

Os **algoritmos de chave única** são também conhecidos como **algoritmos de chave simétrica** e, caracterizam-se por utilizar a mesma chave tanto para a cifragem quanto para a decifragem dos dados, esse método funciona em aplicações limitadas, como as militares, onde o emissor e o receptor podem se preparar antecipadamente para trocar a chave.

Infelizmente, genericamente esse método não funciona muito bem, pois trocar chaves secretas com todas as pessoas a quem nos queiramos enviar uma mensagem é praticamente impossível. Para ilustrar isso, considere o que teríamos de fazer se tivéssemos que enviar um memorando confidencial para acionistas de uma empresa.

Primeiro teríamos de entrar em contato com cada acionista individualmente para que pudessem fazer a troca das chaves secretas. Isso poderia ser feito por telefone, mas, se as mensagens fossem extremamente confidenciais, talvez fosse melhor trocarmos as chaves pessoalmente. Devemos nos lembrar de que precisaríamos fazer isso com todas as pessoas; cada uma teria uma chave secreta separada.

Para aumentar a complexidade desse sistema, também deveríamos lembrar qual a chave que serve para cada cliente. Se as misturarmos, os clientes não serão capazes de ler as nossas mensagens. Obviamente, esse tipo de sistema não é viável para transações comerciais comuns.

5.2.1.2 – *Criptografia de Chave Assimétrica*

Os **algoritmos de chave pública e privada**, também chamados de **algoritmos de chave assimétrica**, utilizam duas chaves: uma pública que pode ser divulgada e outra secreta conhecida somente por pessoas autorizadas.

Em um sistema de chave pública, cada pessoa tem duas chaves: uma chave pública e uma chave privada. As mensagens criptografadas com uma das chaves do par só podem se decriptografadas com a outra chave correspondente. Portanto, qualquer mensagem criptografada com a chave privada só pode ser decriptografada com a chave pública e vice-versa. Como o nome sugere, normalmente a chave pública é mantida universalmente disponível e a outra chave, a chave privada, é mantida em segredo.

O criptosistema inteiro se baseia no fato de que a chave privada é realmente privada. Se um invasor conseguir roubar a sua chave privada, tudo estará perdido. Não importa qual seja a eficiência do algoritmo de criptografia - o intruso vencerá e poderá ler e criar mensagens utilizando seu nome.

ADVERTÊNCIA

Mantenha sua chave privada secreta. Não a guarde em um texto simples no sistema. Se um intruso roubar a sua chave privada, ele poderá assumir a sua identidade e enviar e receber mensagens como se fosse você.

5.2.1.3 - *Assinatura Digital*

A Assinatura Digital é um dos maiores avanços em relação à autenticidade da informação. Como a criptografia por chaves simétricas pode ser utilizada por ambos as lados envolvidos nas comunicações:

Pública >>> Privada e Privada >>> Publica

Podemos assegurar a nossa identidade como autores de determinada mensagem.

Ter duas chaves separadas proporciona outro benefício: a **assinatura digital**.

Se encriptarmos uma mensagem com a nossa chave privada, a única chave capaz de decriptá-la é a chave pública, com isso, todas as pessoas que possuírem essa chave, poderão ler a mensagem e isso não é vantajoso. Por outro lado, como as únicas pessoas que sabem da nossa chave primária somos nos mesmos, está assegurada a nossa identidade como autores dessa mensagem.

Isso é muito importante. Na criptografia com chave pública, cada par de chaves é único. Só existe apenas uma chave pública para cada chave privada e vice-versa. Se isso não fosse verdade, a assinatura digital não seria possível. Um impostor poderia utilizar outra chave privada para criar uma mensagem que pudesse ser lida pela chave pública fornecida.

5.2.1.4 - *Criptografia Combinada de Chave Pública e Criptografia de Chave Simétrica*

Agora vamos ver a combinação dos dois métodos. A criptografia com chave pública é

computacionalmente intensiva e, conseqüentemente, é necessário muito tempo para criptografar uma mensagem com apenas alguns parágrafos.

No entanto, nem tudo está perdido, pois os melhores aspectos da criptografia com chave simétrica e da criptografia com chave assimétrica podem ser combinados, codificando-se a mensagem com o método da chave simétrica e criptografando-se a chave simétrica com o método de chave pública.

Esse método se beneficia da força dos dois tipos de cripto-sistemas: a velocidade da criptografia simétrica e a facilidade dos mecanismos de distribuição de chave do sistema de criptografia com chave pública. Ele resolve o problema de garantir a confidencialidade de uma mensagem, mas como fica a integridade e a não repudiação? Poderíamos simplesmente criptografar a mensagem utilizando a chave privada do emissor, como fizemos antes.

Infelizmente, encontramos os mesmos problemas de desempenho, discutidos anteriormente, com relação a confidencialidade. Para resolver o problema, precisamos introduzir outra ferramenta útil conhecida como **message digest (ou hash)**.

A Message digest é uma função que obtém uma mensagem como entrada e produz um código de tamanho fixo como saída. Por exemplo, se tivéssemos uma função de message digest de 10 bytes, qualquer texto que executássemos através da função produziria 10 bytes de saída, como **dar3ksjudr**.

Devemos nos lembrar de que cada mensagem deverá produzir facilmente uma message digest aleatória, ou seja, qualquer par de mensagens que escolhermos deverá produzir uma message digest específica.

Existem muitos algoritmos de message digest ou hash, mas para que eles sejam úteis a esse propósito (considerados criptograficamente seguros), o algoritmo deverá exibir determinadas propriedades, tais como:

- ***Sem retorno*** - Deverá ser difícil ou impossível determinar a mensagem que produziu uma determinada saída. Isso impedirá que alguém substitua uma mensagem por outra que tenha a mesma message digest.

- ***Aleatoriedade*** - A mensagem deverá parecer aleatória, mais uma vez para impedir que alguém determine a mensagem original.

- ***Exclusividade*** - A message digest deverá ser exclusiva, de modo que a existência de duas mensagens com a mesma message digest seja impossível.

Várias message digests exibem essas propriedade. As mais utilizados são o MD4 e o MD5, e o SHA.

5.3 - ALGORITMOS CRIPTOGRÁFICOS

Conforme já vimos anteriormente os modernos algoritmos de criptografia podem ser classificados em dois tipos de acordo com o tipo de chave que utiliza: os de chave única e os de chave pública e privada.

Os algoritmos de chave única, são também conhecidos como algoritmos de chave simétrica e, caracterizam-se por utilizar a mesma chave tanto para a cifragem como para a decifragem dos dados, o exemplo mais difundido de cifrador computacional de chave única é o **DES** (Data Encryption Standard)**.**

Os algoritmos de chave pública e privada, também chamados de algoritmos de chave assimétrica, utilizam duas chaves: uma publica que pode ser divulgada e outra secreta conhecida somente por pessoas autorizadas, como exemplo de cifrador de chave pública vamos falar sobre o **RSA**.

5.3.1 - DES (Data Encryption Standard)

O **DES** é basicamente uma cifra de substituição que utiliza um caractere de 64 bits. Ele possui uma chave de 56 bits e o seu algoritmo tem 19 estágios. Ele executa uma série de transposições, substituições e operações de recombinação em blocos de dados de 64 bits. Inicialmente, os 64 bits de entrada sofrem uma transposição e são colocados em uma função usando tabelas estáticas de transposição (conhecidas como caixas "**P**") e substituição (conhecidas como caixa "**S**").

Exemplo do funcionamento de uma caixa "**P**":

- "**P**" significa "*permuta"*. Se foram designados 8 bits de entrada, tais como "0, 1, 2, 3, 4, 5, 6, 7" será efetuada uma transposição que irá mudar a ordem dos números. A saída dessa caixa "**P**" poderá ser: "36071245".

Exemplo do funcionamento de uma caixa "**S**":

- "**S**" representa a *"substituição"* dos números por outros números. Supondo-se que o número 0 seja substituído 2, o 1 por 4, o 2 por 5, o 3 por 0, o 4 por 6, o 5 por 7, o 6 por 1 e o 7 por 3. Para uma entrada "01234567" a substituição resultaria em " 24506713".

Os estágios são parametrizados por diferentes funções da chave. A função consiste em 4 etapas que são executados em seqüência. Primeiro, é feita uma transposição de 64 bits dos dados. Os 16 estágios restantes são parametrizados por diferentes funções da chave. O penúltimo estágio troca os 32 bits da esquerda pelos 32 bits da direita (os 32 bits representam uma divisão dos 64 bits). O último estágio é o inverso da primeira transposição.

Em cada uma das 16 interações é utilizada uma chave específica. Antes de se iniciar o algorítimo, uma transposição de 56 bits é aplicada à chave. Antes de cada interação, a chave particionada em duas unidades de 28 bits, sendo que cada uma delas é roteada para a esquerda por um determinado número de bits. Em cada rodada, um subconjunto de 48 bits dos 56 bits é extraído e permutado. O algorítimo, então, executa a transposição final e gera 64 bits.

Esse algoritmo é estruturado de uma maneira que a mudança de qualquer bit de entrada, acarrete em um efeito muito maior em quase todos os bits de saída.

- **DES triplo**

Um documento descreveu uma "máquina de um milhão de dólares" que seria capaz de violar chaves DES rapidamente. Como o projeto dessa máquina só caberia no orçamento de governos

federais e de grandes corporações, muitas pessoas e pequenas empresas começaram a endossar o uso do DES triplo, no qual um bloco de dados é criptografado três vezes com diferentes chaves, como uma alternativa ao DES.

5.3.2 – RC 2; RC 4; RC 5

RC2 e RC4 - Ronald Rivest, da RSADSI (RSA Data Security INC.), projetou essas cifras com tamanho de chaves variável, para proporcionar uma criptografia em alto volume que fosse muito rápido. Um pouco mais rápido do que o DES, essas cifras podem se tornar mais seguras escolhendo-se um tamanho de chave mais longo, eles permitem chaves com o tamanho entre 1 e 2048 bits.

O RC2 pode servir muito bem como um substituto para o DES, pois ambos são cifras de bloco. O RC4 é um outro tipo de cifra conhecido como cifra de fluxo.

Em softwares, o RC2 é aproximadamente 2 vezes mais rápido que o DES, ao passo que o RC4 é 10 vezes mais rápido que o DES. A grande vantagem do RC2 e do RC4 é que eles são exportados com muito mais facilidades pelos Estados Unidos com chaves de 40 bits.

Os algoritmos RC são as cifras mais usadas para os softwares exportados pelos Estados Unidos, mas devemos lembrar que chaves de 40 bits podem ser quebradas usando a técnica de força bruta. Vocês acham que eles iriam deixar exportar coisa boa assim de graça...?

O algorítimo de criptografia **RC 5** é uma técnica mais recente e mais flexível e, tal como o algorítimo DES, é uma técnica de criptografia simétrica, sendo também uma técnica de blocos. Todavia, ao contrário do DES não está limitada a blocos de dimensões fixas, assim como a chave que também não terá a obrigatoriedade de possuir tamanho fixo.

O algorítimo de criptografia **RC 5**, tal como o DES, utiliza a aplicação sucessiva de um algorítimo, contudo, o número de aplicações deste algorítimo não é fixo e, deste modo, pode-se obter um maior grau de segurança, usando um maior número de aplicações.

O **RC 5** é, como se pode deduzir, muito flexível, estando sujeito a uma série de parâmetros que devam ser ajustados às necessidades particulares de cada caso.

A mensagem original é fornecida ao algorítimo sob a forma de dois blocos de "**W**" bits, correspondendo ao alinhamento mais conveniente para o sistema em causa, os valores típicos para "**W**" são: 16, 32 e 64 bits. A mensagem cifrada possui forma idêntica.

Outro parâmetro importante é que o número de aplicações do algorítimo "**R**" pode variar de 1 a 255. Para aplicar "**R**" vezes o algorítimo, vai ser gerada, a partir da chave, uma tabele com: **t = 2 . (R + 1)** blocos de "**W**" bits.

A chave é especificada pelos parâmetros **b** e **k,** onde **b** especifica o número de bytes (octetos) que constitui a chave e **k** é a chave propriamente dita.

É habitual usar a notação RC 5 – W / R / b para especificar uma implementação particular RC 5. Podemos dizer que o RC 5 – 32/ 16/ 7 é equivalente ao DES.

O documento "***The RC 5 Encryption Algorithm"*** contém grandes detalhes sobre o **RC 5** incluindo uma implementação na linguagem "**C**".

5.3.3 - RSA

Este algorítimo matemático, desenvolvido em 1978, deriva do nome de seus inventores, os professores do MIT - Ronald **R**ivest, Adi **S**hamir e o professor do USC Leonard **A**dleman.

O **RSA** usa duas chaves criptográficas, uma chave pública e uma chave privada. A chave é usada para criptografar a mensagem e a chave privada é usada para decriptografar a mensagem, também podendo ser invertida essa seqüência.

A segurança desse método está baseada na dificuldade de fatorar números extensos. Segundo os seus pesquisadores, a fatoração de um número de duzentos (200) dígitos requer quatro milhões (4.000.000) de anos para ser processada. Fatorar um número de quinhentos (500) dígitos exigem 10^{25} anos. Mesmo que os computadores se tornem mais velozes, muito tempo irá passar até que seja possível fatorar um número de quinhentos dígitos e, até lá, poderão escolher a fatoração de um número ainda maior.

5.3.4 - IDEA - International Data Encryption Algorithm

Desenvolvido em Zurique por James L. Massey e Xuejia Lai e publicado em 1990. O **IDEA** usa chaves de 128 bits e é muito forte o que a tornará imune a qualquer técnica ou máquina conhecida atualmente. O **IDEA** é utilizado pelo PGP para criptografar arquivos e e-mail.

A estrutura básica do algorítimo assemelha-se ao utilizado pelo **DES** no que diz respeito ao fato dos blocos de entrada de texto simples de 64 bits serem deturpados em uma seqüência de interações parametrizadas, para produzirem blocos de saídas de textos cifrados com 64 bits. Devido a extensiva deturpação dos bits (em cada iteração, cada bit de saída depende de cada bit de entrada), são necessárias oito interações.

5.4 – SISTEMAS DE PROTEÇÃO

A Internet oferece aos seus usuários uma série de serviços um dos quais e, provavelmente, um dos mais utilizados é o correio eletrônico – "*e-mail"*, do qual estimam-se mais de 30 milhões de usuários da rede, trocando cerca de 4 mil mensagens por segundo.

O correio eletrônico, como todos os demais procedimentos efetuados na Internet, possui algumas vulnerabilidades. As mensagens trafegam por diversos computadores, provedores e demais componentes da rede mundial, antes de chegar ao seu destino. Durante todo o trajeto e enquanto permanece no seu servidor ela pode ser lida e alterada.

Existem diversas formas de mantermos os níveis de segurança e preservarmos a integridade de nossas mensagens e correspondências eletrônicas, dentre alas podemos destacar a Criptografia (da qual trataremos especificamente em um próximo capítulo); o PGP; o S / MIME; o PEM; etc.

5.4.1 – PGP (Pretty Gold Privacy)

Desenvolvido por Philip Zimmerman em 1991, o **PGP** é um pacote completo de segurança de e-mail, bastante utilizado na Internet. Ele oferece confidencialidade, autenticação, integridade dos

dados e não repudialidade. Ele suporta a compressão de mensagens, assinaturas digitais e extensas facilidades gestão de chaves.

A autenticação e a integridade dos dados estão associadas e ambas são conseguidas com a aplicação de uma função de sentido único (one-way hash function) na mensagem e com a cifragem dos resultados antes da transmissão.

O *e-mail,* recurso mais utilizado na Internet, é prático e rápido, todavia não é seguro. Ao enviarmos uma mensagem estaremos nos conectando a um servidor SMTP que a retransmite entre vários roteadores, até ficar armazenada em um provedor, esperando que o destinatário se conecte e o leia. Em qualquer ponto desse trajeto, o administrador de sistemas (ou um hacker, se o sistema não for suficientemente seguro), pode bisbilhotar, ou até mesmo alterar o conteúdo da mensagem.

Se alguém descobrir a nossa senha de acesso, também poderá lê-lo nos nossos provedores antes de nós.

Por fim, qualquer pessoa poderá enviar uma mensagem com a identidade de outro, bastando, para isso, configurar a identidade no programa de *e-mail*.

Mas, existe um programa que ajuda a obter uma transmissão de dados realmente segura, onde apenas o receptor da mensagem poderá lê-la, e ainda terá como saber se o transmissor é realmente quem diz ser e se a mensagem foi alterada pelo caminho. Esse programa é o **PGP**.

O **PGP (Pretty Gold Privacy)** é o programa de criptografia de *e-mail* mais famoso da atualidade. É também um dos programas mais polêmicos da Internet. O seu autor, Philip Zimmerman, sofreu uma série de investigações do FBI e teve de recorrer a grupos de apoio que se formaram na Internet para conseguir pagar seus advogados. O uso deste programa chegou a ser proibido durante dois anos nos Estados Unidos, por infringir a patente do algorítimo RSA. Hoje, porém, o **PGP** é totalmente legal.

Seu poder de criptografia é tanto que o governo americano proibiu o programa de sair do país, pois, representava uma potencial "arma" estratégica. São vários os usos deste programa, sendo muito utilizado como acessório de vários clientes de *e-mail*.

Existem quatro passos fundamentais para a transmissão de uma mensagem utilizando-se o **PGP:**

- ***Assinatura*** (opcional) – Autentica a mensagem de origem, permitindo ao receptor verificar se a mensagem não foi alterada durante a transmissão;

- ***Compressão*** – A aplicação de um algorítimo de compressão, de modo a diminuir o tamanho da mensagem, retirando as redundâncias;

- ***Cifragem*** (opcional) – Consiste na aplicação de algorítimos de cifragem.

- ***Codificação*** (opcional) - Consiste na conversão de caracteres ASC II de 7 bits.

5.4.1.1 – *Segurança e Aspectos Legais do PGP*

Quão segura é uma mensagem encriptada por **PGP**? Podemos afirmar que é muito segura. O **PGP** utiliza o algorítimo RSA de encriptação por chave pública. Um ataque do tipo ***"força bruta"*** ao

RSA é impensável. Estima-se que uma rede de um milhão de computadores Pentiun III levaria cerca de cento e vinte e cinco mil anos para quebrar uma única chave 1024 bits.

Por fim, veremos as questões legais no uso do **PGP.**

Programas que usam encriptação com chaves maiores de 40 bits não podem ser exportados para fora dos Estados Unidos. O **PGP** foi desenvolvido, originalmente, nos Estados Unidos. Todavia, como existem duas versões deste programa, uma americana e uma internacional, a versão internacional foi desenvolvida fora dos Estados Unidos, onde as leis de exportação de programas com criptografia não se aplicam, o que nos permite a sua utilização.

O Brasil ainda não possui nenhuma lei que trate do uso de encriptação de dados. Portanto, programas,empresas ou indivíduos que os use estarão agindo legalmente.

5.4.2 – S / MIME

O **S / MIME** consiste em um esforço de um consórcio de empresas, liderados pela RDSADI e pela Microsoft, para adicionar segurança aos e-mail no formato MIME.

Apesar de tanto o **PGP** quanto o **S / MIME** serem padrões para a Internet, o **S / MIME** deverá se estabelecer no ambiente corporativo enquanto o **PGP** no mundo do e-mail pessoal.

Os certificados digitais são considerados credenciais digitais e têm a mesma função do certificado físico, porém é muito mais barato e rápido. Eles são usados para impedirem a substituição ou fraude de uma mensagem e validar o seu remetente.

Se no certificado convencional, além das pessoas responsáveis em assinar o documento, existe um oficial que reconhece a assinatura em cartório, no certificado digital há uma entidade certificadora que pode ser representada pela própria empresa ou por uma CA – *Autoridade de Certificação*, como por exemplo: "*Verising"; "Nortel"* ou *Cybertrust.*

Existem vários tipos de certificados:

- *Certificados Pessoais* – Contém o nome do portador, seu endereço eletrônico e endereço postal.
- *Certificados de CA* – Estes certificados validam outros certificados, são auto assinados, ou assinados por outra CA.
- *Certificados de Desenvolvedores de Software* – Estes certificados validam as assinaturas associadas a programas.
- *Certificado de Servidor* – Eles tem a capacidade de identificar um servidor seguro, contém o nome da empresa e do DNS do servidor.

O uso da criptografia e dos certificados digitais deixa de ser uma opção para ser uma necessidade em empresas que desejam fazer uso da praticidade da transmissão e recepção de mensagens, sem se expor aos problemas de autenticação e de privacidade.

5.5 - QUESTÕES PRÁTICAS NO USO DA CRIPTOGRAFIA

Vejamos algumas questões de gerenciamento relacionadas ao uso da criptografia:

5.5.1 - Tamanho da Chave

A criptoanálise, ciência da decodificação de cifras, se baseia no fatoramento de números grandes. Conseqüentemente, quanto maior a chave, mais difícil decifrá-la. No entanto, as empresas que conduzem negócios nos Estados Unidos e no exterior são limitadas pelas leis americanas à utilização de chaves de 40 bits em suas aplicações.

Quarenta bits já são o bastante? Depende do que está sendo criptografado; as chaves RC4 de 40 bits podem ser decifradas com uma certa facilidade. Portanto, você não vai quere usá-las para criptografar informações durante um período muito longo.

Apesar de exigir um esforço considerável, a decifração de uma mensagem criptografada com uma chave RC4 de 40 bits, é possível. As chaves de 40 bits podem ser seguras para criptografar ordens de compra ou mensagens de correio eletrônico (que só precisam permanecer secretas até que o destinatário as receba), mas talvez não sejam suficientes para proteger segredos vitais para as empresas.

5.5.2 - Revogação de Certificado

O que acontece quando uma chave privada é comprometida, ou uma chave pública passa a ser inválida? Nesse caso, os certificados deixam de ser confiáveis, pois as informações que eles estão certificando não são mais verdadeiras.

Como podemos impedir que os certificados sejam usados? Muitas autoridades de certificação divulgam, periodicamente, listas de certificados que não devem mais ser considerados válidos, as CRLs (Certificate Revocation Lists). Os certificados dessas listas podem ter espirados ou, o par de chaves associados ao certificado, pode ter sido decifrado.

As CRLs são muito eficientes para verificar a precisão de um certificado em um determinado momento. No entanto, as CRLs não lhe dão qualquer garantia de que um certificado não foi revogado desde sua divulgação. Por essa razão, muitas organizações estão procurando outras soluções para lidar com a verificação de certificados.

5.5.3 - Estrutura de CA

Já falamos sobre CAs e como podem ser "encadeadas" em hierarquias de certificação. Portanto, as grandes organizações podem optar por ter dentro delas várias CAs (uma para o departamento de pesquisa, outra para o departamento de bolsas e assim por diante) e ter uma única CA de nível mais alto para certificar as CAs dos departamentos.

No entanto, manter vários níveis de CAs pode ser complicado. Além disso, ter uma única CA na empresa cria um "único ponto de falha", pois o comprometimento do par de chaves da CA corporativa pode resultar na perda das chaves de todos os funcionários da empresa. Outras empresas optam por uma estrutura plana de CAs, na qual cada CA departamental tem muitas outras CAs parceiras, que correspondem ao outros departamentos da empresa.

É melhor ter uma hierarquia de CAs, na qual o comprometimento de uma única CA pode resultar no comprometimento de todos os certificados da empresa, ou é melhor ter uma estrutura plana, na qual várias CAs devem ser controladas e devem trocar mensagens umas com as outras?

5.5.4 - Fazer ou Não Fazer Caução

Esse é um dos assuntos mais debatidos no que se refere à criptografia. Muitas empresas afirmam que, como a comunicação dos funcionários é propriedade da empresa, a organização deverá ter acesso às chaves dos funcionários, recuperar mensagens (quando houver desligamento de funcionários ou quando eles perderem suas chaves, por exemplo).

Por outro lado, a maior parte dos defensores da privacidade é veemente contra essa idéia, citando a emenda federal que garante os direitos dos funcionários à privacidade. (E no Brasil, como anda isso?).

5.5.5 - O que fazer com todas essas informações

O arquivamento de chaves e de dados criptografados (mensagens de correio eletrônico criptografadas, ordens de compra assinadas,...) é uma questão extremamente difícil. Muitas empresas têm de armazenar informações durante muitos tempo, devido a regulamentos ou outras restrições. Mas, com freqüência, armazenar mensagens ou ordens de compra pode envolver muito mais do que simples manutenção de informações. Considere, por exemplo, o armazenamento de ordens de compras assinadas. Como as assinaturas só podem ser verificadas com a chave pública apropriada, todas as chaves públicas (e suas cadeias de certificação) devem ser guardadas para sempre. Mais uma vez, para grandes empresas, isso pode ser complicado.

5.6 – VANTAGENS E DESVANTAGENS DO USO DA CRIPTOGRAFIA

È lógico que existem vantagens e desvantagens para o uso das técnicas de criptografia, para mantermos os níveis de segurança dos nossos ambientes computacionais. Vale a pena observarmos essas vantagens e desvantagens

- **Vantagens:**
  - Proteger as informações armazenadas e em trânsito;
  - Deter as possíveis alterações indevidas dos dados;
  - Identificar pessoas.

- **Desvantagens:**
  - Não há como prevenir que um intruso
  - Apague todos os seus dados, estando eles criptografados ou não;
  - Modifique o programa, para modificar a chave. Desse modo o receptor não conseguirá decriptografar a mensagem com a sua chave inicial;
  - Acesse o nosso arquivo antes dele ser criptografado.

CONCLUSÃO

Atualmente, nenhum método de criptografia é totalmente seguro. O que os diferencia é a dificuldade de se quebrar a chave e, assim, pessoas desautorizadas terem acesso às informações críticas de uma empresa.

O método ideal para se criptografar uma informação também não é o mesmo para todos. O usuário comum que queira criptografar um *e-mail*, pode utilizar o **PGP.**

O método **DES** pode ser utilizado por usuários que queiram guardar os seus arquivos criptografados, ou, até mesmo, por empresas que queiram transmitir informações pelas filiais, onde possam existir meios seguros para a transmissão das chaves.

O caso mais problemático é o das grandes instituições financeiras e de comércio eletrônico, onde milhares de usuários, todos os dias, enviam suas senhas e números de cartões de crédito pela Internet. Neste caso, o meio mais seguro é o **RSA**.

Embora o RSA também não seja totalmente seguro, a quebra de uma chave RSA é praticamente impossível. A segurança desse método se baseia na dificuldade de fatorar números extensos. Segundo os seus pesquisadores, a fatoração de um número composto por uma quantidade muito grande de dígitos demora um tempo tão grande que se torna quase que impossível, mesmo utilizando um computador de alta velocidade de processamento como ferramenta de apoio.

CAPÍTULO VI

VÍRUS DE COMPUTADOR

CAPÍTULO VI
VÍRUS DE COMPUTADORES

Mantermos a segurança dos dados que trafegam em uma rede de computadores é extremamente difícil, pois, existem milhares e milhares de programas intrusos prontos para atacarem os sistemas e causarem estragos irreparáveis. São os chamados ***vírus***, programas potencialmente destrutivos feitos por alguém e colocados em circulação até atingiram um computador, através de arquivos infectados. São programas pequenos e simples que passam de programas para programas, ou de discos para discos, se alto copiam, fazendo ou não alterações em arquivos ou programas, sem conhecimento e sem autorização do usuário do computador a ser infectado.

Com a popularização da Internet ou das Intranetes nas companhias, a proliferação dos ***vírus*** tomou dimensões ainda mais alarmantes, fazendo com que esses ***vírus*** entrassem na onda da globalização. Se há bem pouco tempo eles invadiam a maioria das máquinas, basicamente pela inserção de disquetes infectados, atualmente eles atravessam fronteiras ancorados em qualquer mensagem de correio eletrônico.

Os sistemas informatizados podem passar a ter um comportamento estranho, não por acidente, mas pela execução de códigos gerados com intuito de danificar ou adulterar o comportamento normal dos softwares. Esses códigos são chamados de ameaças programadas.

Normalmente as ***ameaças programadas*** são chamadas de ***vírus***, mas tecnicamente, existem outras nomenclaturas mais específicas. As diversas ameaças programadas são classificadas pela forma como se comportam, como são ativadas ou como se espalham. Os tipos principais são:

6.1 – VÍRUS

Normalmente chamamos de ***vírus*** a pequenos programas projetados para se replicarem e se espalharem de um computador a outro, atacando programas ou o setor de boot de um disco rígido.

São seqüências de códigos inseridas em outro código executável, de forma que, quando esses programas são ativados, os ***vírus*** também são executados. Como os ***vírus*** não são programas executáveis por si mesmos, sempre necessitam de outro código para que sejam executados.

São variações dos ***vírus***: os cavalos de Tróia, com um mecanismo de ativação (evento ou data) e com uma missão (apagar arquivos, enviar dados, etc.), que se propagam (anexando-se a arquivos e programas). Uma vez ativo, o ***vírus*** pode infectar imediatamente outras partes do computador (outros programas, arquivos, disquetes e setores de disco) ou permanecer residente na memória do computador e, oportunamente, infectar outros programas e disquetes. Normalmente são encontrados em microcomputadores.

Os ***vírus*** malignos podem provocar, principalmente, os seguintes danos:

- Erros no momento da execução de um programa;
- Perda da memória disponível;
- Lentidão para entrar em programas;
- Danos nos dados;
- Danos físicos nos drivers;
- Formatação indesejada das unidades de discos;
- Alocação desnecessária da Memória do Computador.

6.1.1 – Classificação dos Vírus

As classificações dos ***vírus*** são definidas, de uma forma geral, pelos alvos de infecção e de disseminação. Assim, podemos classificá-los como:

- **Vírus de Arquivos ou de Programas** – este tipo de ***vírus*** visam, primeiramente, os arquivos executáveis de programas e de aplicativos.

- **Vírus de "Boot" ou de Sistemas –** estes ***vírus*** visam instruções executáveis específicas existentes nos setores de inicialização dos discos rígidos ou flexíveis.

- **Vírus de Macro –** Estes ***vírus*** visam os programas que suportem documentos e arquivos com macros (como por exemplo: o Word e o Excel).

6.1.1.1 - *Vírus de Arquivo ou de Programa*

Estes ***vírus*** 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"** e outros.

Quando executamos um programa que consistem em um ou mais arquivos executáveis, ele é carregado na memória do computador para ser processado. Se este arquivo estiver infectado, os códigos viróticos também serão processados.

Após a execução, normalmente o programa é liberado da memória, a não ser que seja um programa residente em memória. A maioria dos ***vírus*** de arquivos pode permanecer residente na memória. Quando um ***Vírus de Arquivo ou de Programa*** não continua na memória do sistema após a sua execução, ele é chamado de ***Vírus de Arquivo de Ação Direta.***

6.1.1.2 - *Vírus de "Boot" ou de Sistemas*

Estes ***vírus*** infectam códigos executáveis localizados em certas áreas de sistema do disco. Todo drive de disco, rígido ou flexível, contém um setor de inicialização, e reserva uma parte desses recursos para as informações relacionadas a 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 este pequeno programa que irá indicar ao computador em que parte do disco estão os demais arquivos necessários a inicialização do sistema.

Assim sendo, um ***Vírus de "Boot" ou de Sistemas*** pode se esconder em qualquer tipo de disco, mesmo que ele não seja destinado a inicialização do sistema. Esses ***vírus*** visam se disseminar através de disquetes que são levados de uma plataforma para outra, e que por ventura possam ser esquecidos no driver durante a inicialização.

6.1.1.3 - *Vírus de Macro*

Constituem uma categoria relativamente nova de ***vírus***. As primeiras contaminações trouxeram capacidades inéditas para o mundo dos ***vírus***.

Os *Vírus de Macro*, ao contrário dos tradicionais, podem atacar um mesmo programa em mais de um tipo de plataforma e se disseminam em arquivos de dados que suportem macros dos programas aplicativos.

Pela facilidade de manuzeio na criação e de edição deste tipo de ***vírus***, eles já são a família mais numerosa.

Muitos de nos temos uma visão errada dos ***Vírus de Macro***, pois, cremos que eles sejam feitos da mesma forma que os convencionais, ou seja, em linguagem de baixo nível. Todavia, eles são realmente muito diferentes, tanto que as formas de detecção antigas são inúteis para detectá-los, já que os antivírus anteriores a 1996 não foram programados para verificarem instruções em linguagens de macros, muito menos avaliarem as suas periculosidades.

6.1.2 – Tipos de Vírus

Existem vários tipos de vírus. A seguir relacionaremos alguns desses tipos.

6.1.2.1 - *WORMS*

São programas que se propagam de um computador para o outro em uma rede, sem necessariamente modificar programas nas máquinas de destino. As ***Worms*** são programas que podem rodar independentemente e trafegam de uma máquina a outra através das conexões de rede, podendo ter pedaços de si mesmos rodando em várias máquinas.

As ***worms*** geralmente não modificam outros programas, embora possam carregar outros códigos que o façam (como vírus, por exemplo). Um exemplo de ***worm*** ocorreu em maio de 2000, a VBS / Love Letter e suas variantes, causando problemas em redes de computadores do mundo inteiro.

6.1.2.2 – *BACTÉRIAS*

São programas que geram cópias de si mesmo com intuito de sobrecarregar um sistema de computador. As ***bactérias*** são programas que não causam explicitamente danos aos arquivos. Seu único propósito é a sua replicação. Essa reprodução de ***bactérias*** é exponencial, podendo assumir toda a capacidade do processador, da memória ou do espaço em disco, impedindo o acesso de usuários autorizados a esses recursos.

6.1.2.3 - *BOMBA LÓGICA*

A ***Bomba lógica*** é uma ameaça programada, camuflada em programas que é ativada quando certas condições são satisfeitas. As bombas lógicas permanecem dormentes, ou inativas, em softwares de uso comum por um longo período de tempo até que sejam ativadas.

Quando isso ocorre, executam funções que alteram o comportamento do software "hospedeiro". Geralmente as condições ativadoras de bombas lógicas são: um dia da semana ou do ano; a presença ou ausência de certos arquivos; ou um determinado usuário rodando a aplicação. Uma vez ativada, a bomba lógica pode alterar ou destruir dados, travar o computador ou danificar o sistema.

6.1.2.4 - *CAVALO DE TRÓIA*

Programa que parece ter uma função, mas que, na realidade, executa outras funções.

Análogos ao mito da história grega, os Cavalos de Tróia modernos se parecem com um programa que o usuário gostaria de rodar (como um jogo, uma planilha eletrônica ou editor de textos). Enquanto parece estar executando o que o usuário quer, na verdade, o cavalo de Tróia está fazendo algo completamente diferente, como por exemplo: apagando arquivos, reformatando discos ou alterando dados.

Tudo o que o usuário vê é apenas a interface adulterada do programa que ele queria utilizar. Quando o Cavalo de Tróia é percebido, geralmente já é tarde demais. Normalmente os Cavalos de Tróia são utilizados como veículos para vírus, worms e outras ameaças programadas.

6.1.2.5 – *"TROJAN HORSE"*

São pequenos programas que ocultam os seus reais objetivos sob uma camuflagem de programas úteis ou inofensivos. Um exemplo hipotético de ***"TROJAN HORSE"*** seria um programa escrito, por exemplo, para formatar de forma incondicional o disco rígido oferecido como um duplicador de disco. Isso poderia ocorrer imediatamente ao instalarmos ou executarmos o programa.

Os "***playloads"*** dos ***"TROJAN HORSE"***, na realidade podem ser os mais variados, de acordo com os desejos do seu criador. Normalmente, além da destruição dos dados ou dos sistemas, os ***"TROJAN HORSE"*** podem visar à quebra dos níveis de segurança dos sistemas, através de um programa genericamente chamado de ***SNIFERS*** que rastreiam o sistema atrás de senhas, ou através de programas que transformam o seu computador em cliente de outro de forma oculta.

Ainda que alguns autores considerem os ***vírus*** como um tipo particular de "***TROJAN HORSE***", eles não podem ser classificados como tal, pois, possuem as seguintes características:

- Não possuem instruções que possibilitem a sua alto-replicação;

- São programas autônomos e não necessitam infectar outras entidades (programas, setores, etc), para serem executados;

- Sempre possuem um "***playloads"***, ativados por diversos tipos de gatilhos automáticos, disparados pelos próprios usuários, por seqüências lógicas de eventos, ou por uma data ou período de tempo;

- Não existe uma preocupação primordial de auto preservação após o "***playloads"***, já que não visam à auto duplicação.

Os anti vírus normalmente detectam os ***"TROJAN HORSE"*** e as precauções que tomamos para combater e minimizar os efeitos dos vírus costumam ser eficientes para evitá-los. Todavia os ***"TROJAN HORSE"*** não se limitam às características dos vírus, podendo ser potencialmente mais perigosos e de "***playloads"*** imediatos. Portanto todo cuidado deve ser pouco para prevenir a infecção dos nossos computadores por esse tipo de vírus.

6.1.3 – <u>Estratégias de Prevenção</u>

Quando uma plataforma está infectada é comum o aparecimento de alguns sintomas, tais como: mensagens indevidas, músicas, ruídos, figuras e desenhos, etc. Para um nível maior de certeza e segurança, é essencial manter-se um anti vírus atualizado nos nossos computadores. Para evitarmos problemas deste tipo, sempre é bom evitarmos o uso de disquetes desconhecidos ou, quando não pudermos evitar, devemos testá-los, antes de inseri-los no computador.

Outro aspecto importante que devemos atentar reside no fato de quando recebermos arquivos e mensagens via Internet devemos testá-los antes de utilizá-los.

Para realizarmos esta prevenção podemos nos valer dos ***programas anti vírus*** que são programas capazes de detectar e de retirar os possíveis ***vírus*** das mídias infectadas. Existem vários tipos de programas anti vírus e todos eles tem a mesma finalidade, todavia nenhum deles é 100% infalível.

Uma estratégia preventiva contra os ***vírus de computação*** deve ser feita em dois níveis:

- ***Prevenção de Infecção –*** barreiras de checagem e monitores residentes em memória são as linhas de defesa para evitarmos a contaminação de uma plataforma;

- ***Prevenção Contra Danos*** – devemos utilizar discos de inicialização e "**backups"** que possam neutralizar ou minimizar os danos que podem ser causados pelos vírus dos computadores.

De qualquer maneira a prevenção visa à adoção de mecanismos de defesa capaz de prevenir ou neutralizar a ação desses programas tão danosos aos sistemas computacionais.

CONCLUSÃO

A proliferação dos vírus computacionais é, hoje, uma realidade no mínimo assustadora. Quantas plataformas são infectadas diariamente sem que o seu responsável tenha sequer noção do que está acontecendo. Todavia, nos ambientes computacionais das empresas é inadmissível que fatos desta natureza venham a acontecer.

A participação e a compreensão dos usuários para com os riscos que podem trazer o descaso e a não observação das medidas adotadas para a prevenção da infecção por vírus é de fundamental importância.

Uma política adequada e o gerenciamento dos recursos computacionais são medidas fundamentais para a segurança computacional.

Todavia, devemos mais uma vez observar que segurança não se faz com ações isoladas e sim com um conjunto de medidas que se complementem.

O elo mais fraco da corrente da segurança são os nossos usuários. Faça de cada um deles um parceiro atento à política estabelecida. Não o deixe fora do movimento pela segurança, pois, o descaso é o motivo principal do nosso fracasso!!!

CAPÍTULO VII

ATAQUES E FERRAMENTAS DE ATAQUES

CAPÍTULO VII
ATAQUES E FERRAMENTAS DE ATAQUES

A Internet nasceu em 1969. Após a sua conclusão e estabilização, os pesquisadores confrontaram-se com um fato de real importância: "A Internet não é segura e pode ser facilmente marcada". Atualmente escritores, para amenizar este fato, ressaltam que a tecnologia de segurança empregada naquela época era muito primária. Todavia, podemos observar que hoje em dia a tecnologia de segurança de rede é bastante mais complexa e a Rede Mundial continua sendo fraudada.

Vários são os fatores que contribuem para com a insegurança de Internet, como por exemplo:

- **Falta de Conhecimento** – A falta de conhecimento é uma das principais causas que contribuem para com a insegurança da Internet. Nós acreditamos que aquilo que não conhecemos nunca irá acontecer conosco. Se nos compete a responsabilidade de administrar um Servidor, ou mesmo um ambiente computacional, é melhor não acreditarmos nisso. O conhecimento é simplesmente o aspecto mais importante em relação à segurança.

- **Anonimato –** Outro fator que contribui em muito para com a insegurança é o anonimato, pois, a rede é democrática e dispõe de vários serviços para proteger a privacidade de seu usuário o que dá àqueles mal intencionados a certeza de que este fator lhes é totalmente favorável.

- **Disseminação da Tecnologia –** Hoje, qualquer usuário da rede que pesquise de forma constante, poderá ter a sua disposição às mesmas ferramentas utilizadas pelas organizações governamentais ou pelas empresas especializadas em segurança.

- **Falta de Interesse dos Usuários –** Para a maioria o assunto **segurança** é chato e entediante. Eles acham que segurança na Internet é assunto para especialistas. Até certo ponto, isto é verdade. O provedor deve ter responsabilidade pelos serviços que prestam aos seus usuários. Porém nós sabemos que não é isto o que ocorre na prática do dia-a-dia. As empresas têm receio de se comunicarem umas com as outras e trocarem informações sobre os ataques que sofreram e nunca divulgam as brechas encontradas, como medidas cautelares para as demais empresas.

Como podemos observar, qualquer pessoa pode estar exposta a um ataque.

Esses ataques acontecem, muitas vezes, porque os provedores de acesso são administrados por pessoas que, ou não possuem uma instrução adequada a fornecerem os serviços adequados, ou simplesmente negligenciam nas suas atividades.

Infelizmente, no Brasil não possuímos nenhuma organização que nos mantenha informados sobre os ataques e as suas conseqüências. Embora este tipo de modalidade de crime esteja começando a proliferar no País, nada impede que tentemos combatê-los. Entretanto, nos faltam ferramentas adequadas para fazermos frete a essa prática. As ferramentas são poucas e as que estão disponíveis são extremamente caras.

Outro fator importante é a inexistência de uma legislação sobre este tema. Seria de grande valia a criação de legislações específicas que pudessem combater juridicamente estes procedimentos.

A maioria dos hackers novatos somente passa a ser conhecida quando a mídia noticia a sua captura, pois, eles ainda são muito inexperientes e por isso deixam rastro por onde passam. Mas pouco se sabe dos mais experientes, pois eles são muito cuidadosos nos seus ataques, conseqüentemente, são difíceis de serem encontrados.

Mas, o que os motiva a fazerem esses atos? Os motivos são muitos e podemos classificar alguns deles:

- **Espionagem Industrial** – Ocorre quando um hacker é contratado por uma empresa para roubar e destruir os dados da concorrente.

- **Proveito Próprio** – Ocorre quando existe a possibilidade de, ao invadir, o hacker tirar proveito próprio, tais como: transferências de dinheiro, vantagens em concursos, uso indevido e clandestino de sistemas de telefonia e comunicações.

- **Vingança** – Esta chega a ser clássica. Um ex-funcionário que conhece o sistema pode causar muitos danos aos sistemas de informação se o seu acesso não for cortado no momento adequado.

- **Status ou Necessidade de Aceitação** – A comunidade hacker encontra um sistema razoavelmente seguro e difícil de ser invadido. Tal fato transforma este sistema em verdadeira gincana. A necessidade de ser reconhecido no meio hacker faz com que ele tente insistentemente até atingir o seu objetivo e ser reconhecido no sub-mundo dos hackers.

- **Busca de Aventura** – A tentativa de invasão a sistemas importantes, onde a segurança está em um nível muito alto, ativa o gosto do desafio dos hackers.

- **Maldade** – A invasão e/ou a destruição pelo simples prazer de destruir.

Hoje em dia um fato que tem preocupado muito as instituições e aos profissionais que lidam com as técnicas de segurança é o surgimento de uma nova classe de hackers – "**bad boy script.** A sua inexperiência e a falta de conhecimento específico faz com que este grupo seja tido com uma ameaça muito grave. Suas ações não planejadas e a falta de conhecimento do que poderão causar às empresas é motivo de sérios aborrecimentos. Seus ataques são graves e causam danos irrecuperáveis, pelo uso indiscriminado de ferramentas que eles próprios não conhecem.

7.1 – PRINCIPAIS TIPOS DE ATAQUES

Antes de iniciarmos as definições dos principais tipos de ataques precisamos definir alguns termos importantes para a nossa compreensão. Assim, definiremos os seguintes termos:

- **Ataque –** Ação que compromete a segurança dos dados e das informações de uma organização.

- **Mecanismos de Segurança** – são mecanismos projetados para detectar, prevenir e recuperar o sistema de um ataque de segurança.

- **Serviços de Segurança** – São serviços que aumentam a segurança de um sistema de processamento de dados e de transferência de informações de uma organização. Esse serviço contém ataques de segurança e fazem uso de um ou mais mecanismos para prover tais serviços.

Outro fator importante a ser considerado é que qualquer tipo de ataque sempre terá uma motivação de algum dos tipos acima relatado e passará por uma fase inicial de planejamento criterioso e poderá levar um tempo razoavelmente grande até que se concretize. Durante este planejamento, todos os fatores e as informações encontradas serão analisadas pelo atacante ou grupo de atacantes e serão utilizadas as ferramentas mais adequadas ao ataque.

7.1.1 - Engenharia Social

O que americanos denominam de So*cial Engineerín*g são as relações sociais que *crackers e* até *hackers* fazem, com o objetivo de auxiliar na coleta, pesquisa e análise de informações técnicas de *hardware, software e peopleware* (que desenvolve políticas de segurança) de suas futuras vítimas.

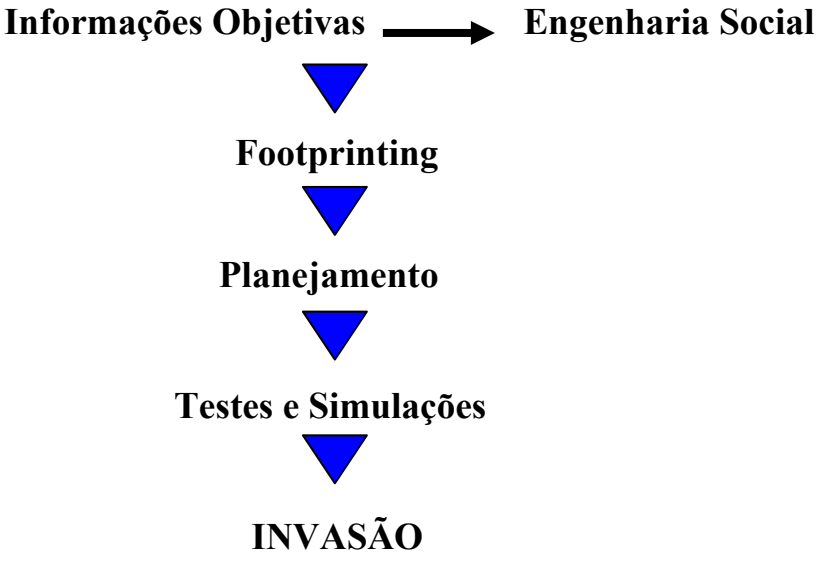
Essa seqüência de ações denomina-se *Footprínting,* que é o primeiro grande passo para um acesso bem sucedido a sistemas alheios.

Um invasor competente coletará o máximo de informações, para correr o mínimo de risco nas suas investidas, e assegurar o máximo de sucesso. Daí, nem sempre as informações objetivas e impessoais, disponíveis e obtidas na Internet e na mídia impressa são suficientes.

Mesmo porque, as informações que ele obtém na rede são, geralmente, referentes aos sistemas *Front-Office* - aqueles que são disponibilizados aos internautas, e não dos sistemas *Back-0ffice* - aqueles sistemas mais vitais, os transacionais, que fazem parte do coração de uma empresa e daí, mais protegidos.

A maior glória para um *cracker* será a de detonar sistemas *Back-Office.* Então, ele necessitará de informações adicionais e complementares, que só mesmo as relações sociais mais humanas propiciam. Nesse sentido, ele trocará mensagens e obterá informações não só através de *e-Mails* e *Chats* no mundo virtual, como também mediante tradicional vivência face a face e dialógica, do mundo real nosso de cada dia.

Só assim o invasor poderá completar todo o seu trabalho de *Footprínting,* que é o primeiro grande passo que antecede o Planejamento, que é o segredo do sucesso de invasões, como demonstramos a seguir.



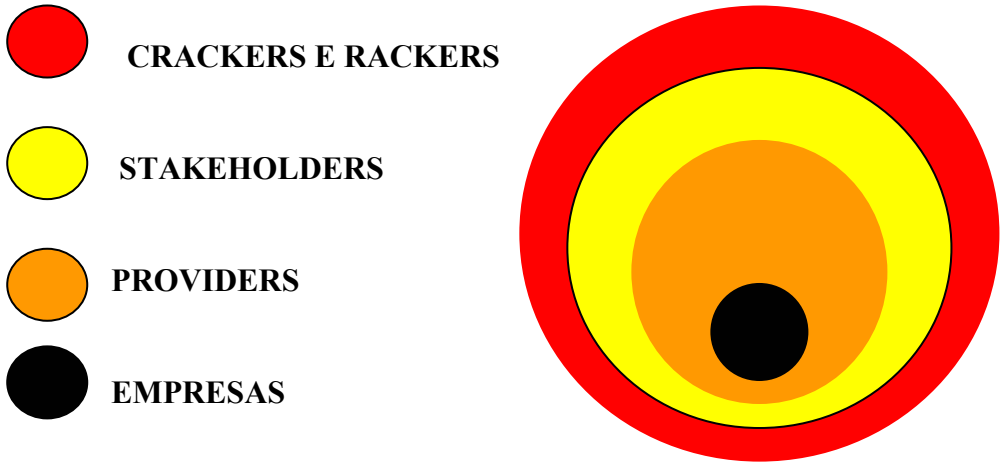
7.1.1.1 - Circulo De Fogo

As informações Objetivas são aquelas obtidas de um ambiente mais externo à empresa, tanto da Internet quanto da mídia impressa, tais como jornais, revistas, livros e catálogos informativos das empresas. Enquanto que o ambiente em que se trabalha a Engenharia Social é o mais interno e íntimo possível da empresa, envolvendo contatos interpessoais.

Se a área de segurança da Internet ainda é incipiente e tem muito a ser desenvolvida, contatos interpessoais e relações humanas no mundo dos negócios têm que ser repensados e *"reengenhariados"*. Tudo isso porque a Internet está disponibilizando e democratizando cada vez mais tudo a todos em rede planetária.

Paradoxalmente, esse fato tende a agredir a integridade, a confidencialidade, a autenticidade e a legalidade que as empresas necessitam, não só para manter a sua segurança, como também para preservar sua própria identidade enquanto ator social.

Como ator social uma empresa conectada está envolvida num **círculo de fogo da Internet**, e daí está sujeito a toda sorte, conforme a figura abaixo:



Nesse círculo da Internet, temos primeiramente os próprios *crackers & hackers,* que normalmente estão a remoto e assim são os agentes mais externos. A princípio, só têm acesso a sistemas *Front-Office e* podem querer acessar os *Back-Office e* demais informações de uma empresa.

Teoricamente, são agentes que têm muito menos acesso a informações das empresas vítimas, que os demais. Mas, são potencialmente perigosos, evidentemente.

Incluímos *hackers* neste grupo, unicamente porque é impossível distingui-los a priori, dos *crackers* nesse círculo de fogo da Internet.

Um alerta que fazemos: não só *crackers & hackers,* mas todos os outros agentes, devem também ser considerados igual e potencialmente perigosos, porque podem ser fontes-chave de informações para invasores.

Analisemos, pois, cada um deles:

- **STAKEHOLDERS**

  São todos os agentes diretamente relacionados com a empresa, em maior ou menor grau de envolvimento com seus negócios. Como STAKEHOLDERS podemos citar: clientes, fornecedores, parceiros e governo. Imagine a troca de informações que ocorre entre os funcionários de sua empresa, com o dos seus *stakeholders*.....

- **PROVIDERS ou PROVEDORES**

  Provedores de Acesso, de hospedagem e *webservices* em geral. Imagine tudo o que você tem na rede; esses seus provedores podem ter igual e facilmente. Imagine depois, uma situação pior ainda: um funcionário deles, com segundas intenções sobre a sua empresa.....

- **EMPRESA**

  Funcionários, dirigentes e acionistas. O maior perigo pode estar dentro de casa. Independentes de serem funcionários, dirigentes e acionistas, estes podem agir objetivamente contra a empresa, conforme os seus mais ocultos interesses. Por outro lado, inadvertidamente, mas principalmente procurando ser solícitos e prestativos com outrem, podem fornecer informações valiosas aos invasores.

7.1.1.2 - *ESTRATÉGIA CONTRA RACKERS*

Que estratégia de sobrevivência e integridade, uma empresa conectada deve seguir, envolvida que se encontra num círculo de fogo da Internet?

Uma estratégia que recomendamos, é aquela baseada na instituição de uma rígida política de segurança, aliada à formação de uma estrutura contingencial de tecnologia de informação. Uma rígida política de segurança que compreenda:

1. Efetivo Controle Segregativo de Acesso Físico e Lógico à plataforma de hardware e software, baseado em ambientes de *mainframes* ou computadores de grande porte, para evitar tanto quanto possível, a disponibilidade indevida da rede a indivíduos fora do controle da empresa;

2. Reengenharia de Instrução e Treinamento de Pessoal, no que tange à comunicação com os stakeholders da empresa - conforme destacamos anteriormente, contatos interpessoais e relações humanas no mundo dos negócios, têm que ser repensados e *"reengenhariados"*.

A nova geração de usuários de micros em rede, que foi educada e treinada para ser mais democrática, solícita e colaborativa, terá de ser *"reengenhariada",* isto é, mudar seu paradigma de comportamento.

Desde telefonista até o mais graduado técnico de Tecnologia de Informação e de um simples mensageiro ao presidente da empresa, todos terão de se habituar a restringir acesso a seus microcomputadores e equipamentos conectados à rede, bem como se sujeitarem às sanções rígidas em casos de desvios às normas.

3. Desenvolvimento e efetivo gerenciamento de um plano de contingência. Estrutura Contingencial da empresa e não somente da sua Tecnologia de Informação, para garantir sua continuidade operacional, em caso de todo o aparato de segurança montado ou parte dele, falhar.

Esse plano, no mínimo, deverá considerar uma configuração dual - um Site Operacional e outro, Backup Site de Processamento e Armazenamento, distante ao máximo permissível do primeiro. Enquanto *o* Backup Site de Processamento e Armazenamento deverá ser o espelho do Site Operacional, este deverá ser subdivido em *Front-Office e Back-Office,* conforme abordamos anteriormente.

Uma menção especial deve ser aqui destacada, as *Providers.*

Para garantir não só a existência, mas principalmente, o funcionamento efetivo dessa Estrutura Contingencial, é condição *sine qua non* que a empresa celebre com as *Providers,* um contrato à altura de suas necessidades de integridade, confidencialidade, autenticidade e legalidade de informações, bem como permanente disponibilidade de seus serviços e estruturas.

Este é o caminho mais seguro possível, para uma empresa não só fazer frente à Engenharia Social dos *Crackers & Hackers,* mas principalmente evitar danos irreparáveis aos seus sistemas. Daí porque doravante contratos **SLA - Service Level Agreement** serão estratégicos para que uma empresa usuária, não só se proteja contra invasor, como também garanta sua continuidade operacional.

4. Auditoria on-line permanente. Se, por um lado, os processos de auditorias são atividades das mais importantes no gerenciamento e no acompanhamento de uma política de segurança computacional, o fato de ela vir a ser executada, também como garantia e prevenção das atividades de engenharia social a transforma em objeto de maior importância. A sua execução cotidiana e rotineira permitirá ao administrador dos recursos de tecnologia da informação, disponibilizada aos diferentes usuários, possa avaliar constantemente a situação em que se encontra a empresa e tomar medidas preventivas e corretivas que eliminem, ou mesmo reduzam as possibilidades da empresa sofrer este tipo de ação por parte de *hackers &crackers.*

Existem dois tipos de ataques principais: O **FOOTPRINTING** e a **VARREDURA.**

7.1.2 – Footprinting

Este ataque é utilizado para conseguir o maior número de informações detalhadas sobre os aspectos de segurança de um alvo previamente estabelecido. O atacante utiliza diversas técnicas de footprinting, na tentativa de descobrir as informações relacionadas com:

- Internet,
- Intranet,
- Acesso Remoto,
- Extranet, etc.

O footprinting se faz necessário para que as informações relacionadas com as tecnologias sejam identificadas e para evitar que, sem o uso de uma tecnologia robusta e de ferramentas adequadas, algumas informações importantes sejam perdidas.

A tabela abaixo mostra a relação entre as tecnologias existentes e as informações que podemos obter por um footprinting.

TECNOLOGIA	INFORMAÇÕES IDENTIFICADAS
INTERNET	Nomes de domínios Blocos de rede Endereços IP específicos dos sistemas atingíveis via Internet Serviços TCP e UDP executados em cada sistema identificado Arquitetura do sistema (Ex.: SPARC versus X86) Mecanismos de controle de acesso Listas de Controle de Acesso (Access Control List – ACLs) relacionadas Sistemas de Detecção de Intruso (IDSs) Enumeração de sistemas (nomes de usuários e de grupos de usuários, faixas de sistema, tabelas de roteamento, informações de SNMP).

TECNOLOGIA	INFORMAÇÕES IDENTIFICADAS
INTRANET	Nomes de domínios internos Blocos de Redes Endereços IP específicos de sistemas tangíveis por intermédio da Intranet Serviços TCP e UDP executados em cada sistema identificado Arquitetura do sistema Mecanismos de controle de acesso Listas de Controle de Acesso (Access Control List – ACLs) relacionadas Sistemas de Detecção de Intruso (IDSs) Enumeração de sistemas (nomes de usuários e de grupos de usuários, faixas de sistema, tabelas de roteamento, informações de SNMP).

TECNOLOGIA	INFORMAÇÕES IDENTIFICADAS
ACESSO REMOTO	Números de telefones – analógicos / digitais Tipos de sistemas remotos Mecanismos de autenticação

TECNOLOGIA	INFORMAÇÕES IDENTIFICADAS
EXTRANET	Origem e destino das conexões Tipos das conexões Mecanismos de controle de acesso

Estas são algumas das principais informações a serem adquiridas por um hacker na sua tentativa de violação. Mas, é importante que saibamos que quanto maior for o número de informações que o invasor adquirir, mais completo será o seu planejamento de ataque e a busca das ferramentas adequadas para o seu intuito.

Este tipo de ataque é o mais comum realizado pelos hackers no mundo todo.

7.1.3 - Varredura

A varredura é um tipo de ataque que tem por objetivo descobrir todas as portas e as janelas e, com isso, identificar os serviços que estão ativos e o sistema operacional do sistema-alvo. Existem dois tipos de varreduras e ambas devem ser executadas, na busca do maior número de informações:

- ***Varredura de Ping***
- ***Varredura de Portas***

7.1.3.1 – *Varredura de Ping*

A Varredura de Ping tem como objetivo identificar um intervalo de endereços IP entre as redes e sub-redes, para determinar se os sistemas alvos estão ativos e confirmar todos os endereços IP envolvidos nas redes e sub-redes.

Este ataque consiste em enviar pequenos pacotes com destino ao sistema-alvo e tentar obter uma resposta capaz de identificar se esse sistema está ativo ou não.

7.1.3.2 – *Varredura de Portas*

Esta varredura consiste em tentar se conectar com os serviços prestados pelos diversos protocolos do sistema-alvo e detectar quais destes sérvios (portas) estão ativas e em execução. Dentre os objetivos de uma varredura de portas estão incluídos:

- Identificar os serviços TCP e UDP ativos no sistema-alvo
- Identificar o tipo de Sistema Operacional do sistema-alvo
- Identificar os aplicativos ou versões específicas de um serviço em particular.

Existem vários tipos de varreduras de portas utilizados pelos atacantes em todo o mundo. A seguir analisaremos algumas dessas varreduras.

- **VARREDURA TCP**

Este tipo de varredura visa se conectar as portas do sistema-alvo e completa um *handshake* de três etapas: SYN, SYN / ACK e ACK. Esta varredura é considerada fraca, pois é facilmente identificada pelo sistema-alvo.

- **VARREDURA TCP SYN**

Este tipo de varredura, também chamada de varredura semi-aberta, pois ela não tem como objetivo a conexão TCP com o sistema-alvo, visa somente identificar os mecanismos de segurança existentes. Ela também é considerada uma varredura fraca, pois, igualmente é de fácil identificação pelo sistema-alvo.

- **VARREDURA TCP FIN**

Esta varredura funciona em pilhas TCP/IP baseadas em UNIX. Ela envia um pacote FIN para a porta alvo, e o sistema-alvo deve devolver um pacote RST para cada porta fechada, ou serviço inativo.

- **VARREDURA TCP de Árvore de Natal**

Esta varredura envia pacotes FIN, URG e PUSH para as portas alvos e o sistema devolve um pacote RST para cada uma das portas que estiverem fechadas.

➢ **VARREDURA TCP Nula**

Esta varredura desliga todos os flags e o sistema-alvo deverá devolver um pacote RST para cada uma das portas fechadas.

➢ **VARREDURA TCP ACK**

Esta varredura é utilizada para mapear os conjuntos de firewall do sistema-alvo e ajuda a determinar se esse firewall executa uma filtragem simples ou complexa dos pacotes enviados.

➢ **VARREDURA TCP de Janelas**

Esta varredura é utilizada para detectar as portas abertas e as portas filtradas / não filtradas do sistema-alvo.

➢ **VARREDURA TCP RPC**

Esta varredura é específica para os sistemas UNIX e é utilizada para identificar e detectar as portas de chamadas aos procedimentos remotos (RPC), bem como o programa e o número das versões correspondentes.

➢ **VARREDURA UDP**

Esta varredura atua enviando um pacote UDP para a porta alvo e espera uma resposta, para saber se ela está aberta ou fechada.

7.2 – FERRAMENTAS DE VARREDURAS E ATAQUES

Existem muitas ferramentas disponíveis tanto para aquisição, quanto grátis na Internet, todas a disposição de atacante e de profissionais de segurança que atuam prestando serviços para as empresas. A seguir mostraremos algumas cujo funcionamento já foi testado exaustivamente.

Estas ferramentas atuam tanto em plataformas de Sistemas Operacionais UNIX e Windows.

7.2.1 – Ferramentas para Sistemas UNIX

Apesar de muitas dessas ferramentas atuarem em múltiplas plataformas estas que nomearemos a seguir foram especificamente criadas para atenderem aos Sistemas em Ambientes UNIX.

➢ ***STROB***

Esta é uma ferramenta de varredura de portas TCP. Ela é uma das mais rápidas e confiáveis que estão disponíveis, pois tem a capacidade de otimizar os recursos de sistemas e de redes varrendo os sistemas-alvo de maneira eficiente e rápida.

➢ ***UDP – SCAN***

Esta é uma das ferramentas de varreduras UDP mais confiáveis, porém ela envia uma mensagem de varredura na maioria dos produtos IDS, fazendo com que não seja uma das ferramentas mais discretas.

- ***NETCAT***

Esta ferramenta poderá executar tantas tarefas que é chamada de **convite suíço**, e tem capacidade de realizar varreduras TCP e UDP.

- ***NETWORK MAPPER (nmap)***

Esta é a principal ferramenta de varredura de portas disponível, e tem a capacidade de executar varreduras TCP e UDP.

7.2.2 – Ferramentas para Sistemas Windows

Assim como as ferramentas supra-citadas estas também poderão atuar em sistemas de outros sistemas operacionais.

- ***NET SCAN TOOLS 2000***

Esta é uma das ferramentas mais versáteis disponíveis atualmente. Ela é capaz de realizar varreduras DNS, WHOIS, varreduras de PING, varreduras de Tabelas de Nomes, Net Bios ou varreduras SNMP. Além de ser capaz de executar uma varredura de portas em uma rede enquanto se executa simultaneamente uma varredura de PING em outra rede.

- ***SUPER SCAN***

Esta é uma ferramenta que realiza varreduras de portas TCP, e tem flexibilidade para especificar e listar as portas IP dos sistemas-alvo.

- ***NTO SCANER***

Esta ferramenta tem uma interface gráfica que executa varreduras de portas TCP e é capaz de capturar *bammer* de portas em estado de escuta.

- ***WIN SCAN***

Esta ferramenta executa varreduras de portas TCP e tem a habilidade de varrer **Redes de Classe C** e a sua saída.

- ***IP EYE***

Esta ferramenta executa varredura de portas TCP, de portas de origem, bem como varreduras SYN, e FIN e de Arvore de Natal. Ela tem uma restrição, pois, está disponível somente para ambientes em Sistemas Operacionais Windows 2000 e varre apenas um host por vez.

- ***WUPS***

Esta é uma ferramenta gráfica que realiza a varredura de portas UDP, em apenas um host por vez, em portas especificadas seqüencialmente.

7.2.3 – Análise das Varreduras de Portas

Após ter completado os ataques anteriormente citados, valendo-se de qualquer uma das ferramentas citadas, o atacante passará a analisar as informações colhidas e planejar as medidas necessárias a execução de seu intento.

O quadro abaixo mostra a ação de cada uma das ferramentas citadas e os ambientes em que atuam.

AMBIENTE UNIX			
PROGRAMA DE VARREDURA	TCP	UDP	FURTIVO
STROB	X		
VARREDURA TCP	X		
VARREDURA DE UDP		X	
N MAP	X	X	X
NET CAT	X	X	

AMBIENTE WINDOWS			
PROGRAMA DE VARREDURA	TCP	UDP	FURTIVO
NET CAT	X	X	
NET SCAN TOOLS	X	X	
PRO 2000			
SUPER SCAN	X		
NTO SCANNER	X		
WIN SCAN	X		
IP EYE	X		
WUPS		X	
F SCAN	X	X	

Observação Importante:

A varredura UDP "NetCat" nunca funciona em ambiente Windows NT. Portanto, não devemos confiar nesta ferramenta quando analisando ambiente neste Sistema Operacional.

7.3 – ATAQUES

Agregadas as informações necessárias o atacante poderá planejar o seu ataque ao sistema-alvo de forma a completar o seu intuito. Existem dois grupos de ataques, cada um com um conjunto de objetivos diferentes, eles são:

- **Ataques Passivos**
- **Ataques Ativos**

7.3.1 – Ataques Passivos

O Ataque Passivo caracteriza-se pela intenção do inimigo em simplesmente observar ou monitorar as transmissões da empresa-alvo. O objetivo do atacante é obter informações indevidas sobre o que está sendo transmitido. Para este intento poderá utilizar duas técnicas de ataque:

- ***Análise de Conteúdo*** - Este ataque consiste na tentativa de descobrir o conteúdo da mensagem.
- ***Análise do Tráfego*** – Essa análise poderá ser feita sobre certas características da mensagem, tais como: padrões de repetições, freqüência e identificação de origem e destino.

Estas informações podem ser úteis para se descobrir a natureza da comunicação. Por sus própria natureza, o ataque passivo não altera o conteúdo dos dados em questão e, portanto, são mais difíceis de serem detectadas.

7.3.2 – Ataques Ativos

Os Ataques Ativos caracterizam-se pela intenção do inimigo em efetuar modificações dos dados nos fluxos das transmissões e / ou nos meios de armazenamento dos referidos dados. Podem ocorrer também a criação de falsos fluxos, com o objetivo de enganar aos receptores. Este tipo de ataque atua de três maneiras nos canis de comunicações:

- ***Interrupção*** – A mensagem enviada pelo remetente não chega ao destinatário, pois o atacante interrompe as comunicações. O atacante pode ou não interceptar a mensagem.

- ***Modificação*** – O atacante intercepta a mensagem e a substitui por outra, elaborada por ele.

- ***Fabricação*** – O atacante insere no canal de comunicações mensagens falsas para o destinatário.

Esses ataques ativos, quando realizados tendo como objetivo as bases de dados, passam a ser classificados segundo os seguintes tipos:

- ***Ataque Mascarado –*** Este ataque ocorre quando o atacante finge ser uma entidade que na realidade não é, e, assim, tentar acessar os sistemas, ou falsificar mensagens.

- ***Ataque de Repetição –*** Consiste em um ataque ativo de captura de dados para uma posterior retransmissão a fim de produzir um efeito não autorizado.

- ***Ataque de Modificação –*** Consiste em modificar parcialmente uma mensagem autentica ou simplesmente atrasá-la ou reordená-la de tal forma a se obter um efeito não autorizado.

➢ ***Ataque de Negação de Serviços*** **–** Consiste em o atacante prejudicar o funcionamento normal de um dispositivo qualquer de gerenciamento das comunicações. Esse tipo de ataque tem por objetivo evitar que um usuário em particular tenha acesso normal a um serviço de comunicações, como por exemplo, a um servidor de mensagens ou arquivos.

➢ ***Ataque de Texto Conhecido*** **–** O atacante passa a ter a sua disposição uma grande quantidade de mensagens criptografadas e, também, mensagens originais equivalentes e, com isso, tenta decifrar as chaves usadas na criptografia.

7.4 – ATAQUES E AÇÕES DOS HACKERS

Existem diversas maneiras de um hacker agir, principalmente através das falhas e brechas de segurança e de serviços, permitindo, conseqüentemente, a violação de sistemas de segurança ineficaz.

7.4.1 – Sniffer

O Snifer é uma ferramenta capaz de monitorar o tráfego de uma rede. Assim como para um administrador de rede isso é necessário, para um hacker esse programa também é muito útil, pois ele poderá se aproveitar desta ferramenta para capturar "logins" e senhas dos diversos usuários.

7.4.2 – Spoof

É a técnica de se fazer passar por outro computador, para conseguir o acesso a um sistema. Existem diversas variantes, tais como: ***Spoofing de IP,DNS(domain number service),*** todavia, todas as variantes resumem-se na substituição do identificador do seu micro por uma de um outro micro qualquer.

7.4.3 – Quebra de Senhas (Password Creaking)

Esta ferramenta consiste em pequenos programas que descobrem as senhas dos usuários válidos dentro de um sistema qualquer. Esta é uma das técnicas mais utilizadas pelos hackers. O método mais comum da utilização destes programas consiste em usar uma relação de palavras previamente estabelecidas **(Word List)** de forma sucessiva, até encontrar a verdadeira senha de acesso.

7.4.4 – Trojans Horses (Cavalos de Tróia)

Esta ferramenta também é composta de pequenos programas que são instalados em seu computador sem você saber e que abrem uma porta de serviços TCP /IP ou uma brecha qualquer em um Sistema Operacional. Esta ferramenta permitirá que um atacante qualquer invada e, posteriormente. Tome conta de seu computador. Os exemplos mais famosos de cavalos de tróia são: "NetBus" e "BackOrifice".

7.4.5 – Mail Bomb (Bombas de e-mail)

Esta técnica, utilizada por muitos hackers, consiste no uso de um script (seqüência de comandos), feitos normalmente em JAVA, que irão gerar um fluxo interminável de e-mails para sobrecarregar a caixa postal de alguém, para que o serviço de e-mail seja interrompido, até o "estouro dessa bomba".

7.4.6 – Denial of Services (Negação de Serviços)

Consiste em sobrecarregar o serviço de um servidor com solicitações intermináveis de serviços. Existem muitas variantes deste tipo de ataque, uma delas foi a responsável pela paralisação dos sites da CNN, Yahoo e ZD Net, no início do ano de 2001.

Um outro tipo de variante desta ferramenta é a instalação de um "Software Zumbi" nos computadores destino que ficam lá até que recebam uma ordem de "bombardeio".

7.4.7 – Port Scan (Scaners de Portas)

Esta ferramenta faz a procura de portas de serviços TCP aberta nas plataformas. Quando ele encontra uma dessas portas abertas, ele a testa por diversos dias em horários diferentes, para saber se ele está realmente aberta e para que o dono da plataforma não perceba isso.

7.5 – PRINCIPAIS TIPOS DE DEFESA

Os hackers quando descobrem que existem defesas contra os seus ataques não se dão por vencidos, e passam a estudar profundamente as defesas encontradas, para então voltarem aos seus objetivos. Algumas dicas a que nos referiremos já foram explanadas no decorrer deste documento, mas nunca é demais referenciarmos estes mecanismos, para que fixemos nossas atividades na busca de níveis de segurança cada vez maiores.

7.5.1 – Senhas

Esperamos que a grande quantidade de detalhes técnicos e a diversidade de assuntos aqui tratados, não nos leve a negligenciar no uso da contra-medida mais trivial e, mesmo assim, a mais importante vistas nessas páginas – **Senhas Fortes.**

Apesar dos rápidos avanços na maioria das áreas da computação, a segurança ainda é bastante comprometida pelo uso inadequado deste item básico. Se, ao terminar de ler estas páginas, você tiver como única idéia para melhorar o nível de segurança da sua empresa a adoção de senhas fortes e de difícil quebra, teremos a certeza de que 90% dos seus problemas com segurança estarão resolvidos.

Assim sendo, o uso adequado de senhas e a confecção de uma política interna de segurança são as principais ferramentas de defesa dos nossos sistemas de informação.

7.5.2 – Equipamentos de Segurança

Toda vez que tivermos um acesso fixo a Internet – através de uma LPCD ou similar, o endereço do nosso computador (IP) passa a ser fixo, e não mais variável como é no acesso discado. Assim sendo, devemos fazer uso de equipamentos que trabalhem em conjunto com eficientes softwares de segurança e que criem barreiras contra acessos indevidos às nossas máquinas, fazendo com que o nosso computador somente receba o que permitirmos, e bloqueando os demais acessos.

Dentre estes equipamentos os mais importantes são: os Roteadores, e os Firewall, com destaque para os Firewall do tipo Proxy, cujas características já foram anteriormente abordadas.

7.5.3 – Atualização de Anti-Vírus

Os anti-vírus mais atuais trazem, além da sua função primária de detecção de vírus, a capacidade de detecção de programas "**back doors**" e de detectores de "**Trojans Horses**". Assim sendo, manter sempre o seu anti-vírus atualizado e fazer varreduras periódicas em todas as plataformas que compõem o seu ambiente computacional é uma prática importante para a garantia do nível de segurança pretendido.

Devemos, ainda, nos lembrar de que a participação dos usuários neste processo é fundamental, pois, as nossas políticas deverão prever medidas que não permitam o uso de ferramentas piratas, disquetes infectados e atentar para o recebimento de e-mails que podem conter uma série de ferramentas utilizadas pelos hackers para invasões.

7.5.4 - Criptografia

O ato de escrever em cifras ou em códigos é a mais importante arma contra a atuação dos hackers, pois existem várias maneiras de se fazer a criptografia. Assim sendo, toda vez que um hacker tentar quebrar o estilo da criptografia, ele terá que começar do zero, pois não existe uma técnica de criptografia igual a outra.

Como podemos observar, aonde pudermos utilizar as técnicas da criptografia, devemos usar, pois grande parte das suas informações estarão preservadas.

CONCLUSÃO

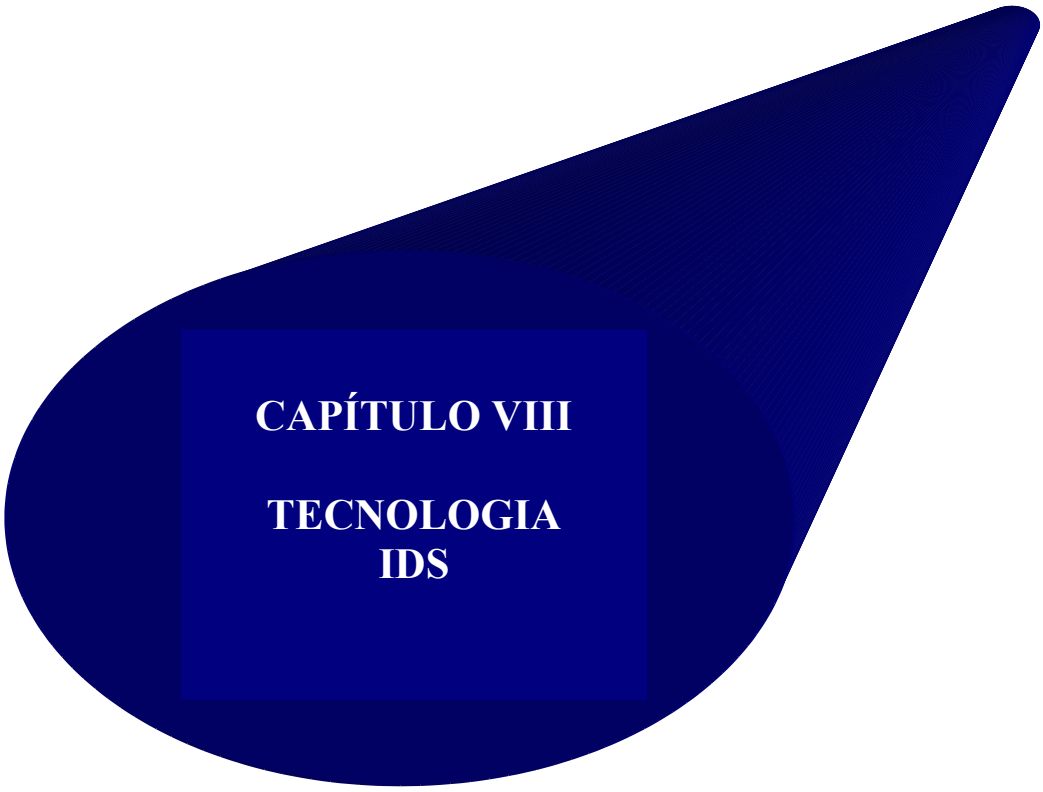
A Internet em seu todo é uma ferramenta de busca de informações das mais importantes de todos os tempos, pois poderemos encontrar todo o tipo de informação que podemos imaginar, mas, assim como essa grande quantidade de informações que circulam na rede nos favorecem em muito, passam a existir muitos perigos também nessas informações.

A quantidade ferramentas de ataques existentes e disponibilizadas na Internet, pode permitir que usuários deste ambiente se transformem em verdadeiros hackers. A abertura das informações para pessoas inescrupulosas e mal intencionadas cria um ambiente dos mais perigosos para as nossas empresas.

A formação de uma nova classe de invasores – os **bad boy scripts** – é uma realidade crescente no mundo inteiro, dispondo de ferramentas as mais variadas e fortes possíveis.

Resta-nos somente adotarmos medidas preventivas e corretivas para salvaguardarmos as nossas instituições.

Assim a adoção de uma Política de Segurança Computacional é de fundamental importância para essa preservação.



CAPÍTULO VIII

TECNOLOGIA IDS

CAPÍTULO VIII
TECNOLOGIA IDS

A maioria dos administradores de rede enfrentarão um evento de intrusão de computador algum dia durante suas carreiras. Ter um plano de detecção de intrusão resultará em notificação de intrusão mais cedo, minimizando as conseqüências e permitindo uma recuperação mais rápida. Algumas empresas fornecem várias ferramentas para detecção de intrusão, incluindo o log de eventos. Este documento discutirá a detecção de intrusão e algumas das ferramentas, que você pode usar como parte de um plano de detecção de intrusão.

É um erro comum, ou apenas um equívoco, pensar que uma *firewall* é o sistema de proteção definitivo para a Internet e o único necessário para implementar uma rede segura.

Na realidade, um firewall é apenas uma proteção passiva, como uma vedação em volta de uma propriedade, com uma ou mais aberturas para permitir a entrada ou saída da mesma. No entanto, essa vedação não pode detectar se a entrada de pessoas é ou não legítima, nem mesmo evitar que alguém tente ultrapassar essa barreira (por exemplo, abrindo um buraco por baixo da vedação, ou saltando por cima).

A utilização de alarmes, câmeras de vigilância, ou detectores de movimento são comuns em muitos locais onde não é possível ter uma pessoa em vigilância permanente, conseguindo-se assim uma forma de proteção mais evoluída, que permite controlar o acesso por parte de pessoas não autorizadas, ou intrusos.

Um *firewall* apenas restringe o acesso a determinadas áreas de uma rede, bloqueando o tráfego que se dirige a pontos não desejados. No entanto, devido às próprias características intrínsecas à sua função, não lhe é possível detectar se todo o tráfego que entra pelas portas de acesso é legítimo. Da mesma forma, também não é possível detectar se alguém está a utilizar mecanismos para contornar ou ultrapassar essa proteção.

8.1 - Detecção de Intrusão (IDS)

Detecção de intrusão é a localização e notificação de atividade sem autorização contra um computador ou rede monitorados. Intrusões podem resultar na mudança de direitos de segurança de usuários e arquivos, instalação de arquivos de Trojan e acesso impróprio aos dados.

A detecção de intrusão é realizada revisando logs de sistemas e implementando firewalls, antivírus e sistemas especializados de detecção de intrusão (IDS). Quando atividade suspeita for notada, você deve investigá-la e descobrir sua origem.

A proteção dos bens ou da informação é, desde sempre, uma preocupação a ter em conta. Pode-se constatar isso verificando que cada vez mais as pessoas procuram meios de assegurar a proteção dos seus bens, sem terem de estar constantemente preocupados com a sua vigilância. Desde sistemas de alarme para imóveis ou veículos, passando por portas e fechaduras reforçadas, de alta segurança, até vigilância por empresas especializadas.

Muitas ferramentas de IDS realizam suas operações a partir da análise de padrões do sistema operacional e da rede, tais como: utilização de CPU, I/O de disco, uso de memória, atividades dos

usuários, número de tentativas de login, número de conexões, volume de dados trafegando no segmento de rede etc.

Esses dados formam uma base de informação sobre a utilização do sistema em vários pontos no tempo, enquanto outras já possuem bases com padrões de ataques previamente montados - permitindo também a configuração dos valores das bases e a inclusão de novos parâmetros. Com tais informações, a ferramenta de IDS pode identificar as tentativas de intrusão e até mesmo registrar a técnica utilizada.

Os Sistemas de Detecção de Intrusão (IDS - Intrusion Detection Systems), são o equivalente a um alarme contra potenciais ameaças externas e permitem detectar eventuais entradas ilícitas na rede das empresas, ou tentativas de ataque aos sistemas que se encontram ligados em rede.

As ferramentas de detecção de intrusão monitoram e relatam atividade maliciosa, incluindo: acesso não autorizado a arquivos e sistemas, ataques de negação de serviço (distribuído), worms, Trojans, vírus de computadores, estouros de buffers, redirecionamento de aplicações, falsificação de identidade e dados, ataques DNS, ataques por e-mail, corrupção de dados e conteúdo e a leitura não autorizada de dados confidenciais.

Os Sistemas de Detecção de Intrusão não substituem os *firewalls*, mas permitem complementá-las. A maioria das tentativas de entrada nas redes empresariais é feita através das portas que estão abertas na *firewall*, para a entrada de **e-mail** ou acesso a servidores **web**.

Neste caso, a proteção por parte da *firewall* é praticamente nula, uma vez que não faz parte das suas funções detectar se o tráfego é malicioso ou completamente normal e inofensivo.

8.2 - Entendendo um sistema de detecção de invasões

As ferramentas para segurança de computadores e redes são necessárias para proporcionar transações seguras. Geralmente, as instituições concentram suas defesas em ferramentas preventivas como firewalls, mas acabam ignorando os sistemas de detecção de intrusão (IDS - *Intrusion Detection System*).

Antes de falarmos sobre o sistema de IDS, temos que definir o que significa uma intrusão. Ela pode ser considerada qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou sistema. Podemos classificar as intrusões em dois tipos:

- **Intrusão devido ao mau uso do sistema** - são os ataques realizados a pontos fracos (conhecidos) do sistema. Eles podem ser detectados pelo monitoramento de certas ações realizadas em determinados objetos;

- **Intrusão devido à mudança de padrão** - são detectadas com a observação de mudanças de uso em relação ao padrão normal do sistema. Primeiramente, monta-se um perfil do sistema. Em seguida, por meio de monitoramento, procura-se por divergências significantes em relação ao perfil construído.

Como a intrusão de mau uso segue padrões bem definidos, elas podem ser descobertas através da comparação de padrões em relação à auditoria do sistema. Por exemplo, uma tentativa de criar um arquivo com *setuis* pode ser detectada pela análise dos *logs* realizados pelas chamadas ao sistema, *call system*.

Uma intrusão devido à mudança de padrões é detectada observando-se divergências significantes em relação à utilização normal do sistema. Pode-se construir um modelo a partir de valores derivados da operação do sistema: uma variável randômica versus valores apurados durante um determinado período de tempo.

Esses valores são apurados a partir de parâmetros do sistema, como utilização da CPU, número de conexões por minuto, número de processos por usuário, entre outros. Uma variação significativa nestes padrões pode ser um indício de intrusão.

Intrusões devido à mudança de padrões são difíceis de serem detectadas. Não existe um padrão fixo que possa ser monitorado; desta forma, devemos trabalhar com aproximação. O ideal seria a combinação de padrões humanos com programas. Assim, o sistema seria monitorado constantemente à procura de intrusão ao mesmo tempo em que teria a capacidade de ignorar as ações de usuários legítimos.

Uma ferramenta de IDS deve possuir algumas características, entre as quais:

- Rodar continuamente sem interação humana e ser segura o suficiente de forma a permitir sua operação em segundo plano. Porém, não deve ser uma caixa preta;
- Ter tolerância a falhas, de forma a não ser afetada por um erro do sistema; ou seja, sua base de conhecimento não deve ser perdida quando o sistema for reinicializado;
- Resistir a tentativas de mudança (subversão) de sua base. Em outras palavras, monitorar a si próprio de forma a garantir sua segurança;
- Causar o mínimo de impacto no funcionamento do sistema;
- Detectar mudanças no funcionamento normal;
- Ser de fácil configuração. Cada sistema precisa ter padrões diferentes, e a ferramenta de IDS deve ser adaptada de forma fácil aos diversos padrões;
- Cobrir as mudanças do sistema durante o tempo, como no caso de uma nova aplicação que comece a fazer parte do sistema;
- E, finalmente, ser difícil de ser enganada.

O último ponto faz referência às prováveis ações no sistema. Eles podem ser classificados nas seguintes categorias:

- **Falso positivo -** é o caso em que ferramenta classifica uma ação como uma possível intrusão, quando, na verdade, trata-se de uma ação legítima;
- **Falso negativo -** ocorre quando uma intrusão real acontece, mas a ferramenta permite que ela passe como se fosse uma ação legítima;
- **Subversão -** acontece quando o intruso modifica a operação da ferramenta de IDS para forçar a ocorrência de falso negativo.

Os IDS permitem assim garantir uma maior proteção das redes empresariais tendo como objetivos:

- Identificar eventuais ataques que a *firewall* deixa passar, de forma legítima (como ataques **http** a servidores **web** ou a servidores de e-mail).

- Identificar tentativas de ataque, detectando, por exemplo, varreduras as portas do firewall.

- Detectar potenciais *hackers* internos à empresa, anomalias na rede provocadas deliberadamente, ou incidentes causados de forma não intencional (mas que podem provocar excesso de tráfego ou congestão da rede).

- Acrescentar um nível de segurança, verificando a existência de falhas ou buracos de segurança nas *firewalls*, tanto em nível de configuração como de fabrico.

8.3 - Tipos de ataques

As razões para utilizar um IDS são essencialmente duas: a proteção da informação e a manutenção da integridade dos sistemas. O desenvolvimento da Internet veio permitir que todos os sistemas e empresas possam estar de alguma forma ligados em rede, à distância de um "click" e expondo-se a uma comunidade de milhões de pessoas espalhadas pelos quatro cantos do mundo.

No entanto, esta interligação traz também alguns riscos. A colocação de servidores disponíveis na Internet implica uma "abertura de portas" aos milhões de pessoas que utilizam a rede de forma anônima.

A sensação de impunidade e o prazer da descoberta leva a que muitas pessoas tentem saber o que existe ligado à Internet. O acesso a servidores internos às empresas, com informação confidencial é normalmente a motivação. O objetivo final poderá ser apenas o de explorar o que existe na rede empresarial, a alteração ou eliminação da informação. Outra razão mais lucrativa é a recolha de informação para venda a terceiros ou para ser utilizada como forma de chantagem.

Mas nem sempre há uma razão aparente para haver tantos ataques a empresas. A maioria deles serve de teste às capacidades dos Hackers e não têm um objetivo direto, se bem que poderão criar graves problemas às empresas vítimas dessas intrusões. Hackers mais experimentados usam várias empresas como ponto de partida para ataques mais avançados, de modo a ocultar as pistas que poderiam levar à sua detecção.

Desta forma e para todos os efeitos, o atacante será a empresa que está a ser usada como ponto de partida, sendo usados os seus recursos para o fazer (largura de banda, servidores).

Alguns *worms* que circularam na Internet (como o NIMDA), utilizaram o conceito de ataque distribuído. Este se propagava e infectava servidores na Internet, que por sua vez procuravam novos servidores para se propagar. O objetivo final era utilizar os recursos dos milhares de servidores infectados para, em simultâneo, atacar sites mundialmente conhecidos.

Normalmente, é possível obter correções (*patches*) para implementar nos servidores, de forma a reparar as falhas de segurança dos servidores e *firewalls,* que são usadas pelos atacantes.

No entanto, estas correções só estão disponíveis algum tempo após a sua descoberta e mesmo assim, nem sempre é possível parar todos os servidores para fazer a sua atualização. Por outro lado, devido à urgência em lançar estas correções, estas não são devidamente testadas em todas as situações e há o risco de comprometerem o funcionamento dos servidores. Por esta razão, os próprios servidores da Microsoft foram atacados 6 meses após a companhia ter lançado uma correção para a falha de segurança explorada no ataque.

8.4 - Modelo Conceitual de uma Ferramenta de IDS

A detecção de intrusão envolve um ou mais das seguintes funcionalidades: alertas, logging, relatórios e prevenção. Os alertas são mensagens de alta prioridade em tempo real enviadas para administradores de rede através do processo de detecção de intrusão para avisá-lo sobre eventos de segurança de alto risco.

Todos os sistemas de detecção de intrusão devem registrar todos os incidentes de segurança percebidos em um arquivo de log, registrando informações como data e hora do evento, risco e outras informações detalhadas. Uma boa ferramenta de detecção de intrusão deve fornecer relatórios de gerenciamento que analisam os arquivos de log e fornecem estatísticas e tendências.

Ferramentas avançadas de detecção de intrusão detectam intrusões e previnem o sucesso dos ataques. Leia a página **I**nternet **S**ecurity and **A**cceleration (**ISA**) Server sobre monitoramento e relatórios para mais detalhes sobre uma aplicação de detecção de intrusão. O planejamento da segurança deve cobrir todas estas quatro funcionalidades na escolha das ferramentas de detecção de intrusão.

Devido à grande variedade de sistemas de IDS, foi proposto o modelo CIDF (*Common Intrusion Detection Framework*). Ele agrupa um conjunto de componentes que define uma ferramenta de IDS. As características desejáveis desses componentes são:

- Devem ser reutilizados em um contexto diferente do qual foram originalmente desenvolvidos, ou seja, devem ser configuráveis de forma a se adaptarem a ambientes distintos;
- Os sistemas de IDS podem ser elaborados em módulos com funções distintas;
- Esses componentes podem compartilhar/trocar informações entre si, via API ou por meio da rede, para uma melhor precisão na identificação de ataques;
- Componentes novos devem automaticamente identificar os demais componentes;
- O grupo de componentes pode atuar mutuamente, de modo a dar a impressão de ser um único elemento.

Segundo a padronização do CIDF, existe um modelo de linguagem para troca de informações entre os componentes, o CISL (*Common Intrusion Specification Language*). Esse formato é referenciado como GIDO (*Generalized Intrusion Detection Objects*). Vejamos cada um deles:

- **Gerador de Eventos (E-box) -** Sua função é obter os eventos a partir do meio externo ao CIDF; ou seja, ele "produz" os eventos, mas não os processa. Isso fica a cargo do componente especializado na função de processamento, que, por sua vez, envia os resultados para outros componentes após analisar os eventos (violação de política, anomalias, intrusão).

- **Analisador de Eventos (A-box) -** Este componente basicamente recebe as informações de outros componentes, analisa tais informações e as envia de forma resumida para outros.

- **Database de Eventos (D-box) -** Sua função é armazenar os eventos e/ou resultados para uma necessidade futura.

- **Unidade de Resposta - (R-box) -** É responsável pelas ações, que podem ser: matar o processo, reiniciar a conexão, alterar a permissão de arquivos, notificar as estações de gerência etc.

- **Comunicação entre Componentes -** A comunicação entre os componentes é definida por uma arquitetura de camadas composta de Gido Layer, Message Layer e Negotiated Transport Layer. Essa arquitetura garante a comunicação entre os elementos, bem como sistemas de criptografia e autenticação. Tais mecanismos estão definidos no COMM (*Communication in the Common Intrusion Detection Framework*).

8.5 - Tipos de IDS

Os Sistemas de Detecção de Intrusão operam normalmente de três formas diferentes:

- **Detecção baseada em assinaturas/padrões de ataques -** Este tipo de detecção baseia-se na escuta e análise do tráfego que passa na rede, detectando indícios de ataques ou atividades exploratórias (tentativas de encontrar falhas ou buracos de segurança para iniciar o ataque).

- **Detecção de Anomalias -** Identifica anomalias na resposta dos servidores ou no seu comportamento. Todos os comportamentos anormais são considerados como suspeitos e sujeitos à análise.

- **Análise dos protocolos -** Analisa os pacotes de informação que passam na rede, identificando se respeitam as regras normais dos protocolos de comunicação (por exemplo, TCP/IP). Parte dos ataques se baseia na utilização de subterfúgios não normais, no nível dos protocolos de comunicação, levando à criação de estados que não foram previstos pelos servidores. Desta forma é possível produzir um ataque com conseqüências imprevisíveis.

Muitos sistemas utilizam mais do que uma destas formas de detecção, de maneira a aumentarem a sua eficácia. Qualquer dos métodos apresentados tem as suas vantagens e inconvenientes, sendo a sua complementaridade importante para obter uma maior precisão.

A precisão pode ser importante para evitar "falsos positivos", ou seja, falsos alarmes. Estes podem ser originados por tráfego considerado suspeito, mas que na verdade é inofensivo. Esta distinção é importante para não criar excesso de alarmes, assim como não deixar passar potenciais ataques, quer sejam externos ou internos.

8.5.1 - Outras características

Além das características essenciais de um IDS existem outras que poderão ser extremamente importantes em algumas situações:

- **Correlação de eventos -** A análise das informações obtidas por vários sensores, em diferentes pontos da rede pode ser extremamente útil para confirmar que se trata de um ataque e ajudar a eliminar potenciais falsos alarmes. Desta forma é possível relacionar informações de diversos pontos em vez de basear a análise num único ponto.

- **Análise integrada dos Logs de outros equipamentos -** A possibilidade de reconhecer os *logs* de equipamentos exteriores ao IDS (como *firewalls*, servidores de e-mail ou web), permite obter informação adicional para consolidar a análise de possíveis ataques ou mesmo anomalias na rede. Desta forma é possível também fazer a análise de segurança de toda a rede a partir de um único ponto central, que reúne as informações de diferentes equipamentos, podendo relacioná-las e apresentá-las de uma forma fácil e rápida de compreender.

- **Performance de sensores -** A performance dos sensores é importante para que não haja perda de pacotes durante a captação da informação na rede. Se não for possível captar toda a informação e analisá-la, corre-se o risco de não identificar problemas ou ataques que estejam a decorrer.

- **Detecção de tentativas de ataques e implementação de alertas -** Deverá ser possível alertar os administradores de rede, de selecionar os eventos por nível de emergência e obter a informação essencial sobre cada evento.

- **Captação de toda a sessão do ataque -** De forma a obter a confirmação de que está a decorrer um ataque e obter toda a informação sobre o mesmo, convém registrar a ação reconhecida como um ataque e também a reação por parte dos sistemas alvo (normalmente servidores).

  Assim, não só será possível saber qual o tipo de ataque que ocorreu, mas também se foi bem sucedido ou não (no caso do servidor não ter sido comprometido). Essa informação é importante para verificar a existência de falhas de segurança ativas e determinar se os servidores estão protegidos contra determinado tipo de situações que estão a decorrer.

8.6 - Criando um plano de detecção de intrusão

Criar um plano de detecção de intrusão significa estabelecer e implantar diretivas de segurança, documentar linhas de base de sistemas e configurar ferramentas que monitoram atividade não autorizada. Criar um plano de detecção de intrusão inclui os seguintes passos:

1. **Inventariar sistemas a serem protegidos**
2. **Criar uma diretiva de segurança**
3. **Proteger os sistemas**
4. **Documentar as linhas de base de sistemas**
5. **Usar e rever os logs de eventos**
6. **Ativar a auditoria**
7. **Implementar ferramentas e métodos de detecção de intrusão**

1. Inventariar sistemas a serem protegidos

Fazer um inventário de sua rede para que você saiba o que está protegendo. É especialmente necessário levantar sistemas sem um log de eventos, NTFS ou participação no Active Directory porque estes sistemas podem ser mais difíceis de serem gerenciados e protegidos. Faça um levantamento dos riscos de incidentes de segurança e documente o que inventariar.

2. Criar uma diretiva de segurança

Os administradores de segurança precisam estabelecer diretivas de segurança por escrito, que descrevem as práticas padronizadas na manutenção da segurança dos sistemas. As diretivas de segurança devem incluir quem pode acessar quais computadores, uso aceitável, diretivas de senhas, restrições de softwares e configurações de segurança padrão para os sistemas.

3. Proteger os sistemas

Uma vez identificado os sistemas de seu ambiente, é crucial certificar-se de que eles estão configurados de forma segura. A Microsoft possui vários recursos de segurança, ferramentas, listas de verificação e how-to's para ajudá-lo a fortalecer a segurança de seus sistemas Windows. Modelos de segurança são a forma preferida da Microsoft para tornar seguras as configurações de segurança de um sistema.

Obs.: A ferramenta Microsoft Baseline Security Analyzer analisa as versões mais comuns de Windows, procurando por vulnerabilidades de segurança e fazendo recomendações a você. O Apêndice A do Security Operations Guide for Windows 2000 Server lista as permissões recomendadas por padrão para estações de trabalho de alta segurança.

Os Guias da Agência Nacional de Segurança americana oferecem recomendações sobre permissões de arquivos e pastas. Considere utilizar um sistema de gerenciamento de patches para manter os seus sistemas atualizados.

4. Documentar as linhas de base de sistemas

O sinal mais comum de uma intrusão está nas alterações no sistema e na mudança não esperada de comportamento de um sistema. Para entender o que é normal você deve examinar os sistemas e o tráfego de rede para criar uma linha base das configurações e atividades.

- **Utilize Modelos de Segurança para documentar e comparar** - Você pode utilizar a ferramenta Security Configuration and Analysis Tool para visualizar e documentar as configurações cruciais de segurança. Você pode usar a mesma ferramenta para comparar a segurança em relação a um modelo pré criado.

- **Verificando e documentando os direitos de usuários e grupos** - Verifique e documente as contas de usuários, grupos, compartilhamentos e permissões. Você pode usar o snap-in Usuários e Grupos Locais dentro de Gerenciamento do Computador ou o utilitário User Manager (NT) para verificar as contas de usuários e grupos.

  Você pode também utilizar os comandos NET USER, NET GROUP e NET LOCALGROUP para listar usuários e grupos. O Windows NT 4.0 Resource Kit e o

Windows 2000 Resource Kit contêm muitos utilitários que ajudam os administradores a auditar direitos e permissões. NETWATCH.EXE é um utilitário interessante que exibe os compartilhamentos e os usuários conectados.

O artigo Microsoft Knowledge Base 137848 detalha como registrar e imprimir uma lista de usuários e grupos e suas permissões utilizando os comandos ADDUSERS.EXE e PERMS.EXE.

- **Verifique os programas e processos ativos -**Use o System Configuration Utility (MSCONFIG.EXE) para visualizar e documentar os programas iniciados automaticamente no Windows 98, Windows ME e no Windows XP.

  Use o Gerenciador de Tarefas no Windows NT, Windows 2000 e no Windows XP para visualizar as aplicações e os processos em execução. O Windows 2000 Resource Kit contém vários utilitários para a visualização de processos, incluindo o PULIST.EXE e o TLIST.

  Use a Lista de processos padrão do Microsoft Windows 2000 ou o Apêndice B do Security Operations Guide for Windows 2000 Server, que lista os serviços padrões instalados no Windows 2000. Muitos administradores acham úteis o PVIEW e o SPYXX para examinarem serviços e processos. Considere usar o utilitário WINDIFF para comparar um sistema ou diretório limpo com um sistema aditado.

- **Netstat e portas TCP -** Documente portas TCP ativas originadas a partir de sistemas monitorados. Use o comando **NETSTAT –a,** para verificar as portas TCP ativas. No Windows XP e Windows 2003, você pode usar o comando **NETSTAT –aon** para verificar que processos estão envolvidos com as portas ativas. Clique aqui para uma lista dos números de portas TCP usadas pela Microsoft ou aqui para uma discussão geral sobre a atribuição das portas TCP.

- **Monitoramento de Rede** - Ferramentas como Microsoft Network Monitor estão disponíveis desde as primeiras versões de Windows, como o Windows for Workgroups 3.11.

  O Network Monitor é uma ferramenta de diagnóstico que captura pacotes de rede examinando-os, traçando-os e gerando estatísticas. O Network Monitor, ou uma ferramenta semelhante é uma peça primária para se criar linhas de base do tráfego de rede.

- **Monitoramento de Performance -** O Windows sempre possuiu um utilitário de monitoramento de performance para analisar e rastrear ocorrências em tempo real. O monitoramento de performance pode ser usado para rastrear objetos, processos e processadores para estabelecer linhas de base.

O Windows 2000 Resource Kit contém um grande capítulo sobre monitoramento de performance. **O Windows NT Workstation Resource Guide** é uma fonte de informação sobre o utilitário NT Performance Monitor, especificamente o Capítulo 9: The Art of Performance Monitoring, Capítulo 10: About Performance Monitor e Capítulo 11: Performance Monitoring Tools. O Capítulo 4- Microsoft Windows NT 4.0 Security, Audit, and Control oferece informações na Tabela 4-4 sobre os contadores para se monitorar por brechas de segurança.

Você precisa entender e documentar as linhas de base para estabelecer os métodos de detecção de intrusão e notificar as atividades não autorizadas quando elas ocorrerem no futuro.

5. Usar e rever os logs de eventos

O Log de Eventos é a ferramenta primária para rastrear a atividade de intrusão em um sistema ou contra um sistema. Os administradores de rede devem verificar os logs em busca de eventos inesperados e investigar atividade suspeita. Os logs de eventos podem ser analisados manualmente ou através de uma ferramenta de análise de logs.

- **Logs de Eventos -** Os sistemas Windows NT, Windows 2000, Windows XP e 2003 compartilham três logs de eventos comuns: Aplicação, Segurança e Sistema.

  Tanto administradores como usuários podem acessar o utilitário Visualizar Eventos no menu Ferramentas Administrativas; o Windows 2000, Windows XP e o Windows Server 2003 possuem um snap-in padrão do Visualizar Eventos.

  Outros logs, como Servidor DNS, Serviço de Replicação de Arquivos e Serviços de Diretório podem estar disponíveis dependendo da plataforma Windows e de como ele foi instalado. Qualquer log pode fornecer evidências de uma intrusão de segurança.

- **Automatizando a visualização de Eventos para múltiplos sistemas** - Se você possui mais de um sistema para monitorar, pode ser difícil ir até cada máquina para monitorar os eventos. O utilitário Visualizar Eventos permite que você abra o log de eventos de máquinas remotas se você tiver direitos administrativos. A Microsoft fornece duas outras ferramentas para a visualização e o gerenciamento de múltiplos sistemas a partir de uma máquina.

- **O EventCombMT** - É um utilitário gratuito da Microsoft usado para a pesquisa de logs de eventos em sistemas remotos entre diferentes domínios, e funciona no Windows NT, Windows 2000, Windows XP e Windows Server 2003. O Capítulo 6-Auditing and Intrusion Detection in Security Operations Guide for Windows 2000 Server tem uma seção sobre o EventCombMT. O download da ferramenta pode ser feita aqui.

- **Microsoft Operations Manager -** Usando um console baseado na Web, o Microsoft Operations Manager (MOM) possui um conjunto completo de recursos que ajudam os administradores a monitorarem e gerenciarem os eventos e a performance de servidores baseados em Windows.

  Ele possui um preço interessante e permite aos administradores de rede centralizarem os logs de eventos e as atividades de gerenciamento de auditoria. Regras pré-determinadas e

diretivas podem ser criadas para gerenciar servidores e para responder aos eventos de servidores que tentam violar estas diretivas.

6. Ativar a auditoria

Apesar de não ser ativada por padrão em nenhuma plataforma Windows, a auditoria pode ser usada para monitorar o sucesso e a falha de tentativas de acesso aos objetos, incluindo logons, acesso a pastas e arquivos, alterações de senhas, uso de aplicações, alterações em direitos de segurança, alterações no registro, alterações em diretivas e desligamentos de sistemas. Os eventos aditados são escritos no log de Segurança.

A Auditoria é uma ferramenta poderosa, mas você deve ter cuidado ao monitorar muita coisa, pois muita informação será capturada e a funcionalidade será perdida. A maioria dos administradores encontram um bom custo/benefício monitorando os eventos de falhas, como uma falha de tentativa de aumentar o privilégio de um usuário, e monitorando todas as atividades críticas, como uma reinicialização de sistema.

Alterações em contas podem ser notificadas ativando-se a auditoria e verificando o log de segurança. Leia os artigos Auditing User Authentication e Auditing User Right Assignment Changes da Base de Conhecimento para maiores detalhes.

A NSA possui uma coleção de Guias de Segurança para Windows detalhando as configurações de segurança de arquivos e recomendações de auditoria. Alguns outros artigos interessantes: How to Monitor Unauthorized User Access in Windows 2000 e How to View and Management Event Logs in Windows XP.

Nota: É necessário utilizar o subsistema NTFS para utilizar toda a funcionalidade da auditoria.

7. Implementar ferramentas e métodos de detecção de intrusão

A detecção de intrusão pode ser feita através do monitoramento de sistemas por atividades inesperadas que diferem da linha de base. Todas as atividades suspeitas devem ser investigadas. Utilize todas as ferramentas acima descritas para comparar e investigar. Outras ferramentas especializadas de detecção de intrusão são úteis em notificar e alertar sobre comportamento suspeito que pode não ser imediatamente notificada por comparações manuais das linhas de base.

- **Firewalls** - A Microsoft tem dois firewalls para monitorar e prevenir tentativas de intrusão.

- **Firewall para Conexão a Internet** - O Windows XP Internet Connection Firewall é um firewall de inspeção de estado de pacotes criado tanto no Windows XP Home como no Windows XP Professional. Ele pode ser usado para prevenir tentativas de conexões não autorizadas entrantes a partir da Internet.

- **ISA Server -** O ISA Server é o principal produto da Microsoft para a detecção de intrusão. Como o sucessor da linha de produtos Microsoft Proxy Server, o ISA ganhou reputação por ser uma ferramenta sólida de segurança de perímetro. Agindo como um firewall e proxy/cache Web, o ISA Server pode filtrar pacotes, circuitos e aplicações e publicar

servidores, podendo ainda ser parte de uma solução de VPN. Várias equipes de auditoria de segurança respeitadas encontraram no ISA Server (pós-Service Pack 1) uma sólida ferramenta de defesa de rede.

Para mais recursos sobre o ISA Server, acesse http://www.microsoft.com/isaserver/techinfo/default.asp. Se você já é um administrador do ISA e procura reforçar a segurança de sua rede e maximizar o seu investimento no ISA, acesse Microsoft ISA Server Partners.

- **Antivírus e Softwares IDS -** Poucas redes podem ser consideradas seguras sem proteção em tempo real de antivírus, tanto em cada estação de trabalho como nos dispositivos do perímetro de rede.

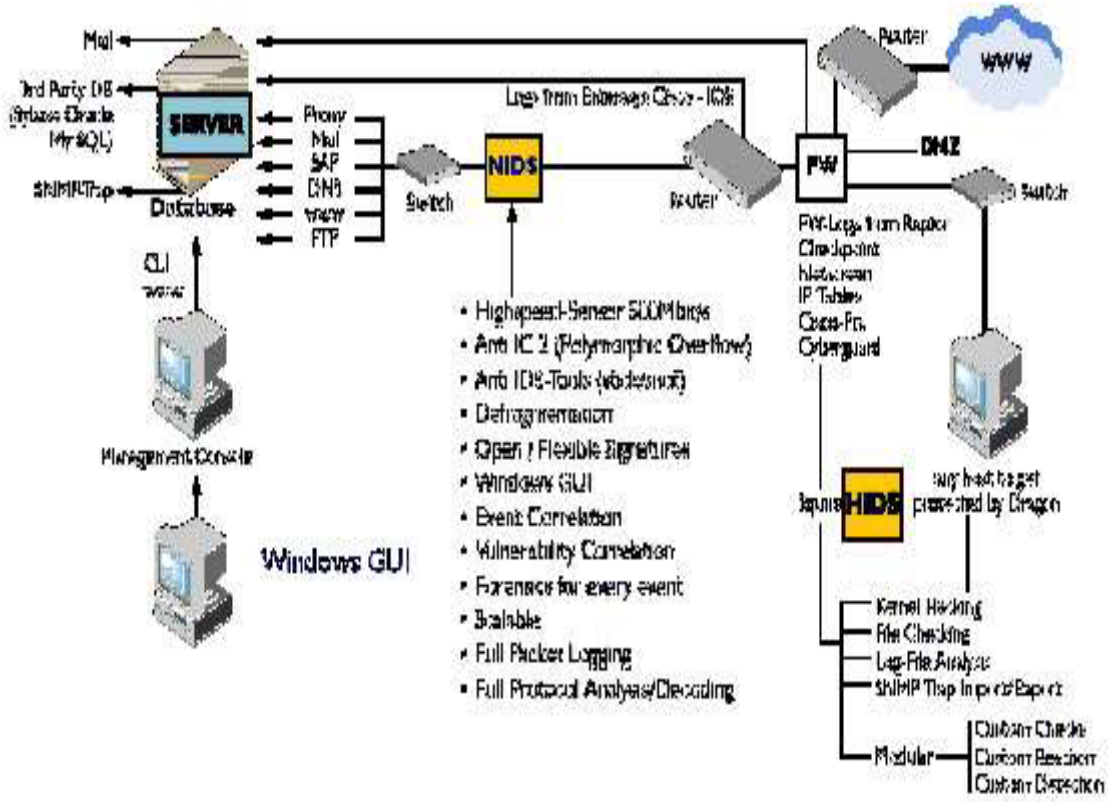
Os fabricantes de Sistemas de Detecção de Intrusão (IDS) estão sempre mudando, portanto a melhor forma de encontrar um é pesquisar na Internet, como no www.msn.com.br, por fabricantes de IDS (use IDS vendors), ou contatar um consultor de segurança.

8.7 - Categorias de Sistemas de Detecção de Intrusos

Os Sistemas de detecção de intrusos caem em duas grandes categorias. Estas são:

- **Sistemas baseados em Rede (NIDS)** - Estes tipos de sistemas são colocados na rede, perto do sistema ou sistemas a serem monitorados. Eles examinam o tráfego de rede e determinam se estes estão dentro de limites aceitáveis.

- **Sistemas baseados em Host (HIDS**) - Estes tipos de sistemas rodam no sistema que está sendo monitorado. Estes examinam o sistema para determinar quando a atividade no sistema é aceitável.



8.7.1 - Sistemas de Detecção de Intrusos baseados em Rede (NIDS)

Sistemas de detecção de intrusos baseados em rede são aqueles que monitoram o tráfego em um específico segmento de rede. Um cartão de interface de rede (NIC) pode operar em um dos dois modos, estes são:

- **Modo Normal** - Onde somente os pacotes que são destinados para o computador (como determinado pelo Ethernet ou MAC Address do pacote) são capturados e carregados para o sistema.

- **Modo Promíscuo** - Onde são capturados todos os pacotes que são vistos no segmento Ethernet onde se encontra o computador.

Um cartão de rede normalmente pode ser trocado de modo normal a modo promíscuo, e vice-versa, usando uma função de baixo nível do sistema operacional para falar diretamente com o cartão de rede para realizar a mudança. Sistemas de detecção de intrusos baseados em rede normalmente requerem que um cartão de interface de rede esteja em modo promíscuo.

8.7.2 - Sniffers de Pacotes e Monitores de Rede

Sniffers de Pacotes e Monitores de Rede foram projetados originalmente para ajudar no processo de monitorar o tráfego em uma rede de Ethernet. Os primeiros destes foram dois produtos; Novell LANalyser e Microsoft Network Monitor.

Estes produtos basicamente capturavam todos os pacotes que eles viam na rede. Uma vez que os pacotes são capturados, várias possibilidades surgem:

- Pacotes podem ser contados. Contando os pacotes que passam na rede, e somando o tamanho total deles durante um certo tempo (inclusive overheads como cabeçalhos de pacote) dá uma boa indicação de como está carregada a rede. LAN Annalyser e Microsoft Network Monitor provêem gráficos da carga ou medidores para mostrar a carga relativa da rede.

- Podem ser examinados pacotes em detalhes. Por exemplo, você poderia querer capturar um conjunto de pacotes que chegam a um servidor de web para diagnosticar algum problema com o servidor.

Produtos que "snifam" pacotes ficaram mais sofisticado atualmente. Programas como **Tcpdump, Ethereal** e as versões mais recentes de Monitor de Rede da NAI, podem desmontar os interiores de vários tipos de pacotes para mostrar que tipo de comunicação está acontecendo dentro daquele pacote.

Uma palavra final sobre sniffers de pacote: Estas ferramentas podem ser usadas para o bem como também para fazer mal. Por exemplo, podem ser usados sniffers de pacote para se descobrir à senha de alguém que tenha se logado via telnet em um sistema Unix, simplesmente capturando os pacotes de telnet endereçados ao servidor que eles geralmente se conectam. Uma vez que o atacante tenha comprometido a sua rede, uma das primeiras coisas que eles poderiam instalar é algum tipo de sniffer de pacotes.

Todos o sniffers de pacote necessitam que uma interface de rede esteja em modo promíscuo. Só em modo promíscuo, todo pacote recebido pelo NIC será passado para a aplicação de sniffer, incluindo pacotes de outras estações e pacotes de broadcast. O sniffer de pacotes regularmente requer privilégios administrativos na máquina que é usada como um sniffer de pacote, de forma que o hardware do cartão de rede possa ser manipulado para estar em modo promíscuo.

Outro ponto para considerar é o uso de switches, em lugar de hubs, em uma rede. Note que os pacotes recebidos em uma interface de um switch não são sempre enviados a outras interfaces do switch. Por isto, um ambiente de rede totalmente configurado com switches, em lugar de um ambiente com hubs (único segmento), estará geralmente imune ao uso de sniffers de pacote.

8.7.2.1 - Detecção de Intrusos baseados em Rede: A Evolução do Sniffer de Pacotes.

Infelizmente, do ponto de vista de segurança, um sniffer de pacotes é muito limitado. A tarefa de capturar o pacote na rede desmontá-lo, e analisá-lo manualmente baseado no conteúdo do pacote, é de longe, muito demorado, até mesmo para uma equipe de especialistas de rede super treinados.

E se nós tivéssemos algum software que automatizá-se o processo para nós (afinal de contas, é para isso que os computadores foram feitos, não é?). Isto é, basicamente, e exatamente o que um sistema de detecção de intrusos baseado em rede (Network Intrusion Detection – NIDS) faz.

Aqui estão exemplos que alguns tipos de detecção de intrusos podem executar:

1. Examinar os pacotes que atravessam a rede;

2. Nos pacotes legítimos, permitir que eles passem (logando-os talvez, para futura análise);

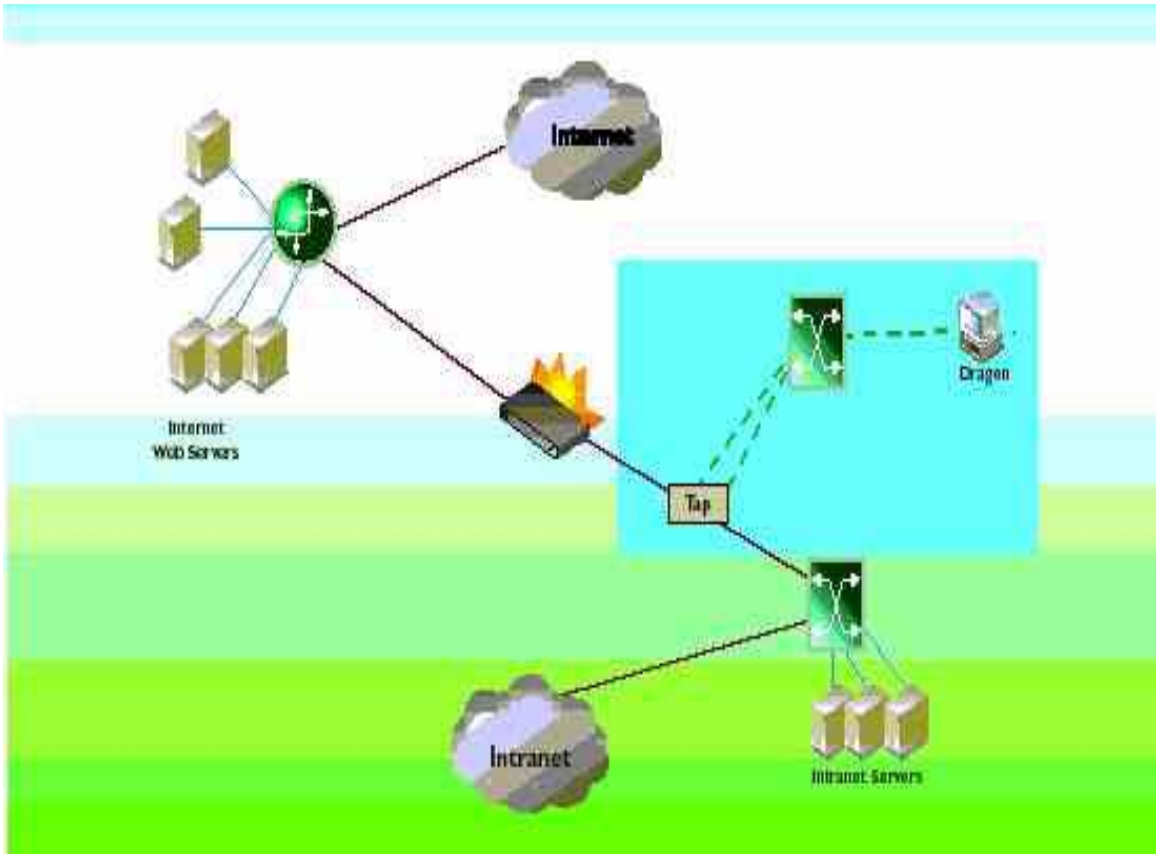
3. Num pacote que pareça quebrar a segurança ou integridade de um sistema, efetuar resposta automática para o fechamento da sessão.

4. Monitorar o reconhecimento da rede (Port Scans), pois toda vez que um cracker deseja comprometer um sistema, antes disso ele necessita reconhecer as vulnerabilidades do sistema.

5. Monitorar conexões válidas para ataques bem conhecidos. Tendo acesso um servidor de web na porta 80 (web - http) poderia ser visto como uma atividade relativamente inofensiva, mas algumas tentativas de acesso são na realidade ataques deliberados, ou tentativa de ataques. Por exemplo, um acesso como **"GET /../../../etc/passwd HTTP/1.0"**, é provavelmente um mau sinal e deve ser bloqueado.

6. Identificar "spoofing de IP" (se disfarça de outro endereço IP) de vários tipos. O protocolo de ARP que é usado para converter endereços de IP a endereços de MAC é freqüentemente um alvo para ataques. Enviando pacotes de ARP forjados em cima de um Ethernet, um intruso que obteve acesso a um sistema pode fingir estar operando como um sistema diferente.

Quando atividade não desejada é detectada, o sistema de detecção de intrusos baseados em rede pode entrar em ação, tanto como interferindo com o tráfego do provável intruso, como reconfigurando um firewall para bloquear todo o tráfego que vem do computador ou da rede do provável intruso.



8.7.3 - Detecção de Intrusos baseados em Servidores (HIDS)

Uma vez que um pacote de rede chegou ao servidor, o qual era o seu objetivo e após ter passado pelo firewall e pelo detector de intruso baseado em rede (NIDS), ainda há disponível uma terceira linha de defesa. Isto é chamado de detecção de intrusos baseados em servidores (**H**ost **I**ntrusion **D**etection – **HIDS**).

Os dois tipos principais tipos de detecção de intrusos baseados em host são:

- **Monitores de rede**. Estes monitoram conexões de rede que chegam ao host, e tentam determinar se quaisquer destas conexões representam uma ameaça. Conexões de rede que representam alguma tentativa de intrusão são alarmadas.

  Note que isto é diferente da detecção de intrusos baseados em rede (NIDS), este só olha para o tráfego de rede que está chegando com destino ao servidor, e não todo o tráfego que passa a rede. Por isto não requer modo promíscuo na interface de rede.
- **Monitores de integridade**. Estes monitoram arquivos, sistemas de arquivos, diretórios, ou outras partes do próprio servidor procurando por tipos particulares de atividades suspeitas que poderiam representar uma tentativa de intrusão ou comprometimento do sistema.

8.7.3.1 - Monitorando as Conexões Entrantes

É possível monitorar na maioria dos servidores, os pacotes que tentam ter acesso ao servidor antes que esses pacotes sejam passados para a camada de rede do próprio servidor. Este mecanismo tenta proteger um servidor interceptando pacotes que chegam ao servidor antes que eles possam fazer qualquer dano.

Algumas das ações que podem ser tomadas incluem:

- Descobrir conexões que tentam abrir sessões TCP ou UDP em portas que não são autorizadas, como tentativas para conectar a portas onde não há nenhum serviço. Isto é freqüentemente um indicativo de um possível cracker tentando reconhecer as vulnerabilidades do servidor em questão.

- Descobrir o mapeamento das portas abertas. Novamente, este é um tipo de ataque que deveria ser gerado um alerta , e se possível alertando um firewall ou modificando a configuração do endereço IP local para negar acesso ao intruso.

8.7.3.2 - Monitorando Atividades de Login

Apesar dos melhores esforços dos administradores de rede, e os mais recentemente softwares de detecção de intrusos, ocasionalmente um intruso se moverá sorrateiramente e conseguirá se logar em um servidor usando algum tipo de ataque desconhecido. Ou talvez um atacante tenha obtido uma senha (password) por outros meios, e agora tem a habilidade para se logar remotamente no sistema.

Procurando por atividade incomum em um sistema é o trabalho para HIDS que monitoram os logs de autenticação. Este tipo de monitores de login alertam o administrador de sistema a atividades que são incomuns ou inesperadas, tais como, um usuário comum receber privilégios de administrador às duas horas da manhã de domingo.

8.7.3.4 - Monitorando Atividades de Administrador ou Root

O objetivo de todos os intrusos é obter o superusuário (root) ou acesso de administrador no sistema que eles invadiram. Sistemas bem mantidos e seguros que são usados como servidores de web e bancos de dados normalmente terão pequena ou nenhuma atividade pelo superusuário, excluindo as horas planejadas para manutenção de sistema.

Felizmente, crackers não acreditam em manutenção de sistema. Eles raramente aderem a janelas de tempo de manutenção agendadas e freqüentemente trabalham em horas estranhas do dia. Monitorando-se qualquer ação executada pelo usuário de root ou administrador, inclui-se mais uma linha de defesa ao sistema.

8.7.3.5 - Monitorando os Sistemas de Arquivos

Uma vez um intruso chegou a invadir um sistema (e apesar de suas melhores esperanças, e os melhores esforços dos sistemas de detecção de intrusos, não se pode evitar completamente a possibilidade de que um dia um intruso chegará a invadir seu sistema), então eles começarão a mudar os arquivos no sistema.

Por exemplo, um intruso experto poderia querer instalar um sniffer de pacotes, ou modificar alguns dos arquivos de sistemas ou programas para desabilitar alguns dos métodos de detecção de intrusos.

A instalação de um software em um sistema normalmente envolve a modificação de alguma parte daquele sistema. Estas modificações normalmente levarão a forma de modificar arquivos ou bibliotecas no sistema.

Alguns programas agentes foram projetados para detectar qualquer mudança no sistema de arquivos, alertando o administrador de sistema sobre estas mudanças.

Por exemplo, as seguintes ações podem ser tomadas para prevenir qualquer alteração:

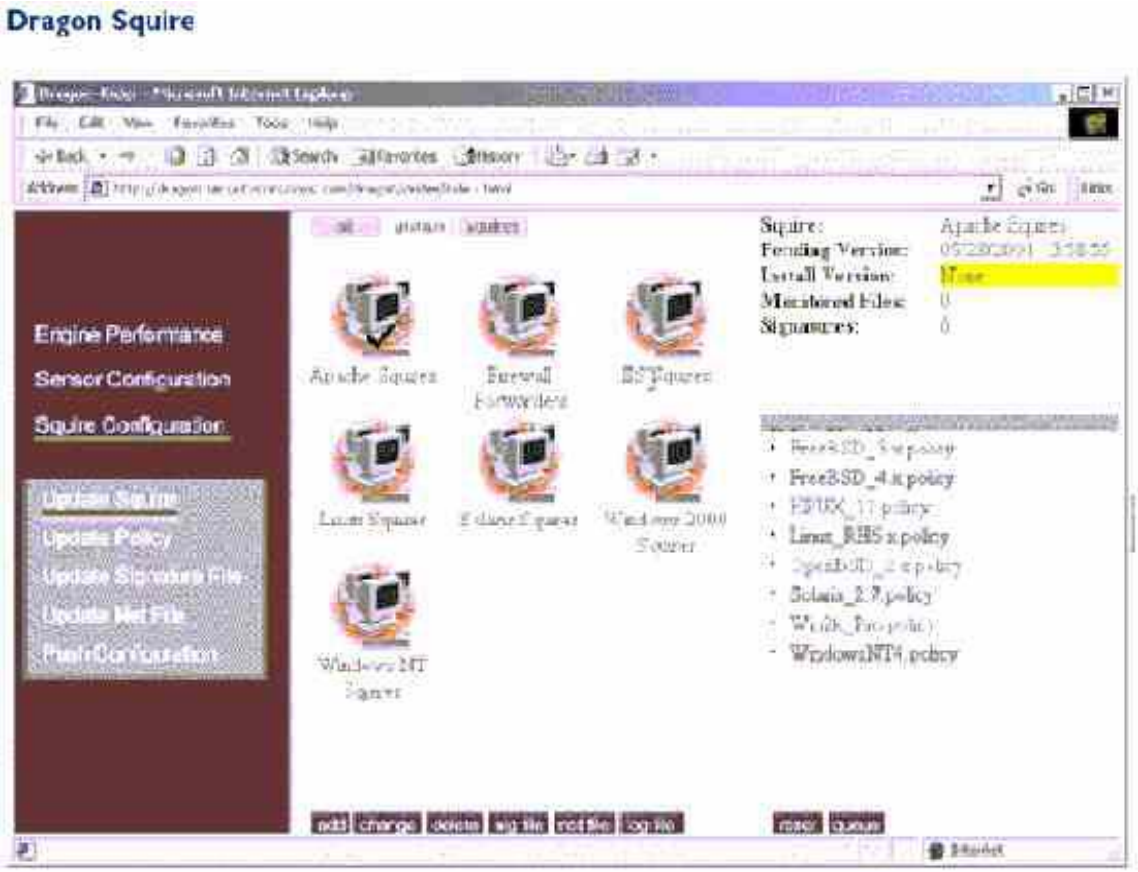
1. Crie um MD5 ou outro checksums criptografado de todos os arquivos críticos do sistema, e armazene estes em um banco de dados. Quando um arquivo mudar, seu checksum mudará.

2. Armazene a data e hora de criação ou data e hora de modificação de todos os arquivos críticos do sistema. Procure qualquer mudança neste "timestamps".

3. Mantenha um registro de qualquer programa no sistema que seja executado como super usuário. Se quaisquer destes mudar, ou se são instalados novos, ou algum seja apagado, então há um problema.

Exemplo de Solução HIDS – Dragon Squire

Neste contexto a Enterasys apresenta seu **Host Intrusion Detection** (HIDS), o **Dragon Squire,** que tem algumas funcionalidades de um monitor de rede bem como acentuada característica de um monitor de integridade.



Para mais informações consultar:

- **Ataques à Microsoft** - http://www.cnn.com/2000/WORLD/europe/10/27/usa.microsoft/
- **Roubo de cartões de crédito:** http://www.cnn.com/2000/TECH/computing/03/13/creditcard.steal.idg/ http://news.bbc.co.uk/1/hi/business/2774477.stm
- **SQL Worm** -http://www.cnn.com/2003/TECH/internet/01/27/worm.why/index.html
- **Vulnerabilidades várias** - http://www.cert.org/incident_notes/
- **Riscos associados** - http://www.idg.net/go.cgi?id=682235
- **Dúvidas freqüentes sobre IDS** - http://www.ticm.com/kb/faq/idsfaq.html
- **Conhecendo o inimigo** - http://www.enterasys.com/products/whitepapers/9012849.pdf
- **Exemplos de ataques e detecção** - http://www.rtsn.pt/html/downloads/ids_meth.pdf
- **Justificar Investimento em IDS** - http://www.securityfocus.com/infocus/1621

CONCLUSÃO

É possível, enquanto usando as ferramentas mais atualizadas que estão disponíveis, proteger-se contra virtualmente todo tipo de ameaça que é atualmente conhecida. Infelizmente, ameaças novas e furos de segurança em algum pacote de software estão sendo descobertos diariamente.

É importante em qualquer ambiente saber que tipos de ameaças você poderia estar enfrentando. Esteja atento a qualquer furo de segurança potencial em seu sistema, e se preocupe em prevenir ataques contra estes.

Por exemplo, um servidor de web que é conectado à Internet e colocou-se atrás de um firewall pode estar razoavelmente protegido da maioria dos ataques, mas um programa de CGI no servidor poderia expor uma vulnerabilidade.

Preste especial atenção e assegure-se que aquele programa CGI confere e valida todos os comandos e dados de entrada antes de processar. Um programa de detecção de intrusos entre o firewall e o servidor de web pode ser configurado para descartar qualquer acesso que for suspeito.

Deste modo é muito importante um sistema de alarme na rede, que avise quando da presença de algum tráfego de pacotes suspeitos e/ou de prováveis vulnerabilidades nos sistemas operacionais e aplicativos de inter/intranet.

Não há rede totalmente segura. A sua rede já foi, está sendo, ou será atacada. Não há como fugir, o que se pode fazer é aumentar as barreiras de segurança para diminuirmos os riscos.

CONCLUSÃO FINAL

O Centro Nacional de Segurança para Computadores (NCSC – *National Computer Security Center*), uma agência do Departamento de Defesa Americano (DoD - *Departament of Defense*), publicou em 1985, um documento intitulado "*Department of Defense Trusted Computer System Evaluation Criteria*", também conhecido como "*Orange Book*" (livro laranja, devido à cor laranja de sua capa). Embora, originalmente, tenha sido escrito para sistemas militares, atualmente, é utilizado pelas indústrias de computadores. Atualmente, o NCSC é chamado NSA (*National Security Agency*).

O *Orange Book* tem até hoje fortes influências na indústria de computadores e estabelece os padrões e exigências para os sistemas seguros que são aprovados pelo DoD. Para que qualquer órgão do Governo Federal Americano possa adquirir um sistema de computação, um nível mínimo de segurança como especificado no livro laranja, deve estar implementado para esse sistema. O livro laranja tornou-se um padrão comercial de uso geral, pois, de um lado os fabricantes começaram a utilizar seus critérios para classificar seus produtos, e de outro, os compradores passaram a dispor de um esquema que permita uma melhor avaliação da segurança fornecida pelos produtos.

O DoD elaborou os critérios para a classificação da segurança dos sistemas de computação, tendo em vista três objetivos principais:

- Fornecer aos fabricantes um padrão, definindo os aspectos de segurança que deveriam ser incorporados a seus produtos. A idéia do DoD era, com isso, incentivar o desenvolvimento de sistemas largamente disponíveis, satisfazendo requisitos de segurança, com ênfase na prevenção contra a revelação não-autorizada de informações, para aplicações sensíveis;

- Prover aos órgãos membros do DoD, uma métrica para ser usada na avaliação do grau de confiança que pode ser atribuído a um sistema de computação que será utilizado no processamento de informações classificadas ou outras informações sensíveis;

- Fornecer uma base para a definição dos requisitos de segurança nas especificações de aquisição de equipamentos.

Este documento leva em consideração cinco aspectos de segurança:

- A política de segurança do sistema.
- Os mecanismos de contabilidade / auditoria do sistema.
- A operacionalidade do sistema de segurança.
- O ciclo de vida do sistema de segurança.
- A documentação desenvolvida e atualizada sobre os aspectos de segurança do sistema.

Um nível de segurança, no livro laranja, indica se um computador possui um conjunto pré-definido de características de segurança.

Desta definição, são extraídos os 6 requisitos básicos, usados para avaliar a segurança de sistemas de computação: quatro deles definem o que deve ser providenciado para controlar o acesso às informações e dois preocupam-se em como avaliar se um sistema de computação realmente garante o controle de acesso.

REQUISITOS DE SEGURANÇA

Os seis requisitos básicos são:

➢ **Política de Segurança:** O sistema deve implementar uma política de segurança explícita e bem definida. Deve existir um conjunto de regras que são seguidas pelo sistema, para determinar quando um dado indivíduo, devidamente identificado, tem permissão para acessar um objeto específico devidamente identificado;

➢ **Rótulos (Marcação):** Rótulos de controle de acesso devem ser associados aos objetos relacionados com a política de segurança. Deve ser possível marcar todos os objetos com um rótulo que identifique, de forma confiável, seu nível de sensibilidade e os modos de acesso associados a ele;

➢ **Identificação e Autorização:** Os indivíduos devem ser apropriadamente identificados. O acesso a qualquer informação é baseado em quem está acessando e quais classes de informação estão autorizados a acessar. Junto com a identificação são guardadas informações sobre o nível de autorização do usuário. As informações de identificação e autorização devem ser mantidas de forma segura pelo sistema de computação e devem ser associadas a todos os elementos ativos que executem alguma ação relevante para a segurança do sistema;

➢ **Registro de Eventos / Contabilização:** Informações para auditoria (em *logs*) devem ser seletivamente mantidas e protegidas para que as ações que afetem a segurança possam ser rastreadas para identificação do responsável. Além disso, o sistema deve permitir a escolha dos eventos a serem registrados para minimizar o tamanho dos *logs* e garantir eficiência na auditoria. Os *logs* devem ser protegidos contra alteração ou destruição não autorizadas;

➢ **Garantia / Confiabilidade:** O sistema de computação deve conter mecanismos de hardware/software que possam ser avaliados independentemente e que forneçam garantias suficientes de que o sistema cumpre os requisitos, anteriormente explicados;

➢ **Proteção Contínua:** O sistema deve ser permanentemente protegido contra reconfigurações ou qualquer alteração não-autorizada. Nenhum sistema de computação pode ser considerado seguro, se os mecanismos que garantem a segurança puderem ser violados. Deve-se dar uma atenção especial a esse requisito, quando forem realizadas atualizações ou reconfigurações do hardware/software do sistema.

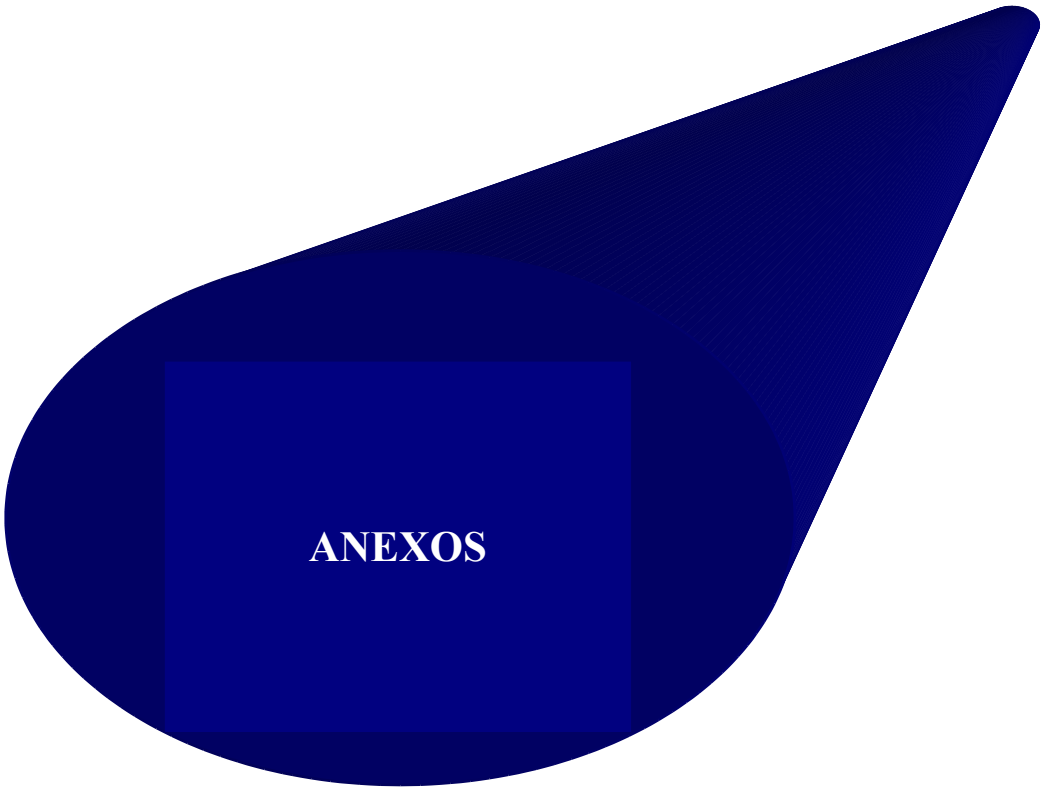
Esses seis requisitos básicos formam a base para a classificação estabelecida no *Orange Book*.

A agregação de todos esses conhecimentos é de fundamental importância e nos permitirá construir uma **POLÍTICA DE SEGURANÇA COMPUTACIONAL** em um nível bastante elevado.

Tenho a convicção de que não esgotei o assunto, mesmo porque ele é vasto e altamente dinâmico. Certamente ao finalizar esta obra, vários dos assuntos aqui tratados já sofreram modificações radicais, todavia, espero ter chamado a atenção daqueles que direta ou indiretamente com os aspectos de segurança que envolvem as nossas empresas e incentivado a todos ao constante estudo, na busca de soluções que nos permitam conviver com um pouco mais de tranqüilidade.

Se todos usassem as suas criatividades, competências e saber em proveito da humanidade, certamente teríamos um mundo melhor e com menos diferenças sociais e econômicas. Infelizmente existem os que usam o saber para destruir o que levamos horas construindo.

Nossa luta é árdua, mas haveremos de vencê-la!


ANEXOS

TROJANs HORSES

Nos dias atuais, podemos observar uma grande incidência de invasões a computadores tanto das empresas como pessoais, que se valem deste tipo de vírus computacional, chamados de **Trojans Horses**.

As empresas especializadas na construção de antivírus têm buscado incessantemente desenvolver ferramentas para evitar novas invasões, todavia, nem sempre conseguem se antecipar no lançamento das ditas ferramentas e, muita das vezes fica a mercê destes vírus, infectando nossos computadores e nos impossibilitando de realizarmos nossas atividades nos nossos computadores.

Mas o que são, na realidade esses **Trojans Horses**? Como eles infectam os nossos computadores? Como identificá-los? Quais os procedimentos a serem adotados para a sua remoção?

Este artigo tem por finalidade orientar os diversos usuários da Internet no reconhecimento e no uso de algumas ações para identificar e retirar estes vírus.

O que são Trojans Horses, como eles infectam nossos computadores.

Os **Trojans Horses** são programas destinados a facilitarem as invasões dos computadores, criados por pessoas que se valem do uso da Internet para promoverem este tipo de atividades. Eles são chamados normalmente de “hackers e crackers”.

Estes programas trabalham com a arquitetura cliente/servidor e fazem do seu computador um servidor de dados para o criador e/ou utilizador deste **Trojan,** permitindo que o hacker tenha acesso direto ao seu computador e “veja” tudo o que nele estiver armazenado. Ex: Senhas, número de documentos, CPF, Cartões de Crédito, etc...

De posse destes dados, o hacker/cracker os utiliza, fazendo qualquer tipo de atividade que estes documentos permitam (compras, desvio de dinheiro, acesso indiscriminado às instituições financeira, etc) como se fosse você, e o pior, sob a sua responsabilidade jurídica.

O seu computador somente será infectado por um **Trojans Horses** se você, por descuido ou por falta de conhecimento, for conivente com isto, ou seja, o não uso de um programa de antivírus atualizado, o descuido com as suas senhas, o uso de senhas inadequadas e fracas, o uso de programas pegos em sites não confiáveis, o recebimento de e-mails de origem duvidosa e a sua abertura e outros comportamentos inadequados são os principais motivos e origens das contaminações dos computadores por todos os tipos de vírus existentes.

Reconheça, de forma simples, se o seu computador tem um Trojans Horses.

Se você perceber um comportamento diferente em seu computador, tal como: erro de teclado, dificuldade de acessar páginas na Internet, aparência diferente do monitor, e outras anomalias, desconfie...seu computador pode estar infectado.

Execute os procedimentos abaixo e tenha a certeza, ou não de uma infecção por vírus:

1) ***Caso esteja conectado à Internet, desconecte imediatamente;***

2) Execute a verificação de seu computador valendo-se de um antivÍrus o mais atualizado possível. Caso não tenha busque um na Internet e execute a verificação. Alguns sites possuem estes antivírus gratuitos.

3) Caso ainda persista a dúvida de uma possível infecção proceda da seguinte forma:

a. *– Vá para o "PRONPT DO DOS"*
b. *– Digite o comando:* NETSTAT –AN (tudo em letra minúscula) e de "enter"
c. *– Vai aparecer uma tela com o seguinte formato*:

C:\>netstat -an

Conexões ativas

Proto	Endereço local	Endereço externo	Estado
TCP	**0.0.0.0:12345**	**0.0.0.0:0**	**LISTENING**
TCP	**0.0.0.0:12346**	**0.0.0.0:0**	**LISTENING**
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3069	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3072	0.0.0.0:0	LISTENING
TCP	**200.255.207.39:12345**	**127.0.0.1:1028**	**ESTABILISHED**
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	0.0.0.0:3010	*:*	

Esta tabela mostra todas as conexões TCP/IP ativas em seu micro computador, com quem e onde o seu micro está trocando informações na Internet.

Repare nas linhas acima que estão sendo utilizadas as portas **0.0.0.0.12345** e **0.0.0.0.12346,** portas estas que, segundo as regras do protocolo TCP/Ip, não são utilizadas e isto lhe indica que realmente o seu equipamento está infectado.

4 - Além deste teste de conexão, você deve examinar o registro do Windows, para tal siga os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em* – **EXECUTAR** *e tecle "*enter**";**
c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**
d) *Aparecerá, em seguida uma tela do editor do registro com seis (6) chaves abaixo:*

- **HKEY_CLASSES_ROOR –** registro de todas as extensões de arquivos registrados no Windows, além dos programas associados.

- **HKEY_CURRENT_USER –** informações sobre o usuário que está utilizando o computador no momento, tais como: desktop, preferências, configurações específicas, etc).

- **HKEY_LOCAL_MACHINE –** todas as informações das configurações de "hardware" e "software" instalados no Windows estão aqui, inclusive as possíveis modificações feitas pelo seu invasor (***back doors)***, caso o seu computador esteja infectado.

- **HKEY_USERS –** registro de usuários cadastrados no computador e as suas especificações (perfis dos usuários).

- **HKEY_CURRENT_CONFIG –** mostra as configurações temporárias dos programas que estão sendo executados no momento.

- **HKEY_DYN_DATA –** mostra todos os "drivers" instalados em seu computador, pois eles ficam aqui registrados, além das configurações "plug and play".

Agora que você já tomou conhecimento com as instruções iniciais necessárias ao reconhecimento de um **Trojans Horses**, vamos tratar especificamente de cada um deles, logicamente dos mais utilizados, e ensinar como reconhecer e como retirá-los.

I – BACKORIFICE

Este é um **Trojans Horses** bastante utilizado e tem por finalidade manter aberta uma porta de serviços do TCP/IP, para que o seu invasor tenha acesso constante ao seu computador.

Para localizar e eliminar este **Trojans devemos** seguir os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em* – **EXECUTAR** *e tecle "*enter**";**
c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**
d) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services**
e) *Procure por algo relacionado com um arquivo chamado:* **windll.exe, exe~1, yerfucked.exe,** ou algum outro arquivo que ao seu ver esteja estranho neste diretório.
f) *Apague estes arquivos e reinicie o seu computador.*

II – NETBUS

Este **Trojan** é o mais utilizado e tem por finalidade disponibilizar a "net bios" se seu computador para o seu invasor e, assim, dar a este invasor privilégios de administrador em seu equipamento.

Para localizar e eliminar este **Trojans** devemos seguir os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em* – **EXECUTAR** *e tecle "*enter**";**

c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**
d) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services**
e) *Procure por um comando do tipo DOS, como por exemplo:* **"/nomsg"** ou **"/noad".**

f) *Observe que talvez tenha sido criada uma "sub-*chave" *para este propósito. Neste caso é muito importante apagar primeiro a "sub-chave" para depois apagar o comando.*
g) *Reinicie o seu computador.*
h) *Se o* **NETBUS** *estiver rodando na sua máquina, talvez você não consiga reiniciar o seu micro na tela inicial do seu Windows –* **INICIAR / DESLIGAR.** *Dai você vai ter que resetar o seu equipamento, mas não esqueça de fechar o editor de registro.*
i) *Procure, também por uma "dll" chamada "***keyhook.dll"** *no seu diretório:* **Windows \ System** ou simplesmente **Windows,** *e a apague***.**
j) T*alvez algum "shareware" que você possua pare de funcionar, pois a maioria delas usa esta "dll". Você pode reinstalar o "software" novamente, ou apenas fazer um "backup" desta "dll" e, após reiniciar o micro, colocá-la no local original novamente.*

III – SOCKETS DE TROIE

Este **Trojan** é muito utilizado e possui algumas variações. Assim sendo devemos ter muito cuidado com a sua retirada.

Para localizar e eliminar este **Trojans** devemos seguir os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em –* **EXECUTAR** *e tecle "*enter**";**
c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**
d) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services.**
e) *Procure o comando:* **"Load MSchv32 Drv = C:\windows\system\mschv32.exe".**
f) *Apague***-**o
g) *Vá para* **HKEY_CLASSES_ROOT \ Directsokets** *e procure por "***Directsoketctrl=$A4D5#FFF"** *apague-o também.*
h) *Uma forma de saber se este* **Trojan** ainda está rodando no seu equipamento é a seguinte:
   - *Aperte em conjunto as teclas "*crtl + alt + del" *e verifique a atividade de um programa chamado "***mschv32.exe**" *este é o programa que roda este* **Trojan.**

i) *Reinicie o seu computador.*

IV – SOCKETS DE TROIE vrs 2.0

Este "upgrade" do **Trojan "SOCKETS DE TROIE"** *é extremamente perigoso, pois possui um vírus que inocula o computador da vítima. Nesta versão não é utilizado o "***mschv32.exe**" *mas sim três (3) outros arquivos diferentes, o que dificulta consideravelmente a localização. Estes arquivos são:*

- **C:\windows\rscload.exe**
- **C:\windows\system\mgadeskdll.exe**
- **C:\windowssystem\csmctrl32.exe**

Se você ainda tiver dúvida se eliminou estes **Trojan,** poderá seguir os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em –* **EXECUTAR** *e tecle "*enter**";**
c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**

d) *Utilize o seu "mouse" e siga o caminho:* **HKEY_CURRENT_USER \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services**
e) *Apague a ocorrência: "***load mgadesk.dll = c:\windows\system\mgadesk.dll"**
f) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services**
g) *Apague a ocorrência:* **"load rscload = c:\windows\rscload.exe"**
h) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services**
i) *Apague a ocorrência:* **"load CSMCTRL32 = c:\windows\system\csmctrl32.exe"**
j) *Reinicie o seu micro.*

V – MASTER´S PARADISE

Este **Trojan** é muito complicado e requer muita atenção para retirá-lo, pois ele modifica os arquivos "**sysedit.exe**" e "**keyhook.dll**", *que vem com o Windows, por isso você será obrigado tomar algumas medidas iniciais.*

Para localizar e eliminar este **Trojans** devemos seguir os procedimentos abaixo:

a) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
b) *Clique em* – **EXECUTAR** *e tecle "*enter**";**
c) *Digite "***REGEDIT"** (tudo em minúsculas) *e tecle "*enter**";**
d) *Utilize o seu "mouse"e siga o caminho:* **HKEY_LOCAL_MACHINE \ Software\ Microsoft \ Windows \ Current Version \ Run** ou **Run Services.**
e) *Procure uma sub*-chave de nome estranho, pois este **Trojan** não usa um nome específico e a apague.
f) *Depois de apagar esta chave, apague os arquivos:* "**sysedit.exe**" e "**keyhook.dll**".
g) *Reinicie o seu micro.*
h) *Instale, novamente, agora os arquivos* "**sysedit.exe**" e "**keyhook.dll**". *O arquivo* "**sysedit.exe**" *você pode pegar no CD do Windows 95/98 e o* "**keyhook.dll**" *você reinstala o "software" que parar de funcionar.*

VI – ICQTROJEN

Este **Trojan** renomeia o executável do ICQ, para "**ICQ2.exe**" e se instala como "**ICQ.exe"** no diretório do ICQ. Quando o usuário se conecta a Internet, o "***netdetect"*** do ICQ carrega o **Trojan** e este, por sua vez, carrega o "**ICQ2.exe"**, não levantando suspeitas ao usuário.

O **ICQTROJEN** utiliza uma porta alta do Windows, ficando em listing, ele usa o mesmo padrão das transferências utilizando o File Transfer Protocol (FTP).

Uma maneira muito prática de verificar se o seu computador está infectado por este **Trojan** é:

a) *Pressione "*crtl + alt + Del*" e verifique a existência de dois ICQs e um, certamente, será o* **Trojan.**
b) *Para resolver este problema, basta ir ao diretório do ICQ, e apagar o "***ICQ.exe".**
c) *Renomeie o"* **ICQ2.exe**" como "**ICQ.exe"**
d) *Reinicie o seu computador*

VII – ICQ KILLER

Este famoso "flooder" para ICQ, que muitas pessoas têm em seus computadores, para forçar outros usuários a fechar o ICQ, é um **Trojan**, muito utilizado e famoso entre os usuários dos "chats".

Este **Trojan** abre a **porta 7789**, pela qual o "hacker" que tiver infectado um usuário qualquer de Internet por este **Trojan**, terá total acesso ao HD de quem estiver infectado, novamente com um funcionamento padrão das transferências utilizando o File Transfer Protocol (FTP).

Para se ver livre deste **Trojan,** basta que quando você estiver no ambiente Windows:

a) *Pressione "*crtl + alt + Del*" e verifique a existência de dois "***Explorer***" rodando.*
b) *Marque o segundo "***Explorer***", e comande "***finalizar tarefa"*** (este é o executável que abre a **porta 7789)**.
c) *Vá para aa tela inicial do seu Windows* - **INICIAR***;*
d) *Clique em* – **EXECUTAR** *e tecle "*enter**";**
e) *Digite "***REGEDIT"** (tudo em minúsculas**);**
f) *Clique em* "**Procurar**", digite "**c:\windows\system\explorer.exe"** *e mande procurar por este arquivo.Ao aparecer, apague-o.*
g) *Depois vá para o diretório* "**c:\windows\system"** *e apague o arquivo* **"Explorer.exe" .**
h) *Reinicie o seu computador*

Como você pode ver, com um pouco de trabalho podemos desinfetar os nossos computadores da presença nefasta dos **Trojans**, porém, é sempre mais inteligente e menos trabalhoso evitar que este tipo de constrangimento nos atinja, sem esquecermos os perigos que isto significa. Para tal, algumas medidas básicas podem e devem ser adotadas, como forma de prevenir tais infecções:

- Tenha sempre instalado em seu equipamento um bom antivírus;
- Mantenha este antivírus atualizado (no mínimo três vezes por semana);
- Não forneça a sua senha de acesso à Internet a ninguém, em hipótese alguma;
- Esteja sempre alerta ao comportamento do seu equipamento (tela, configuração de teclado, velocidade de processamento, etc.);
- Evite dar informações sobre o seu equipamento e Sistema Operacional, para estranhos;
- Tenha cuidado com as propagandas e os sites que não ofereçam segurança;
- Evite dar informação sobre os seus documentos pessoais via Internet (Identidade, Endereço, CPF, número de Cartão de Crédito, telefone, etc.);
- Se necessitar fazer alguma compra utilizando a Internet, faça-a em sites que lhe ofereçam os maiores níveis de segurança;
- Tenham cuidados especiais com os e-mail que você recebe, principalmente os de correntes(use um Anti –Span);
- Tenha cuidados especiais quando navegar pelos "chats de bate papo".

Estas são medidas básicas para o uso seguro da Internet, porem, você pode adotar medidas adicionais, buscando proteger seu equipamento em um nível maior, buscando instalar programas que monitoram e evitam que seu equipamento se infectado por estes programas. Sugiro que você entre nos sites abaixo e busque os seguintes programas:

- **NOBO –** previne a infecção por BACK ORIFICE – www.centroin.com.br

- **BPS –** Monitora a existência de 15 **Trojans** diferentes e executa a remoção dos mesmos – www.mantel.com.br/iw

Se necessitar qualquer contato, favor enviar um e-mail para: tlgosorio@uol.com.br.

Prof Dr. Tito Lívio Gomes Osório.

ANEXO II
FERRAMENTA DE REMOÇÃO DO W32.BLASTER.WORM

O Symantec Security Response desenvolveu uma ferramenta de remoção para limpar infecções do W32.Blaster.Worm.

Notas Importantes:

- O W32.Blaster.Worm explora a vulnerabilidade do RPC do DCOM**.** Esta vulnerabilidade está descrita no Boletim de Segurança da Microsoft MS03-026 e a correção está disponível nesse local. Você deve fazer o download e instalar a correção. Em muitos casos você terá que fazer isso antes de continuar com o processo de remoção. Se não for possível remover a infecção ou evitar a reinfecção seguindo as instruções abaixo, você deve fazer o download e instalar a correção primeiro.

- Devido à maneira como o worm funciona, pode ser difícil conectar-se a Internet para obter a correção da vulnerabilidade, definições de vírus ou a ferramena de remoção antes que o worm desligue o computador. Foi reportado que, para usuários do Windows XP, a ativação do firewall do Windows XP pode permitir que sejam feitos o download e a instalação da correção, e a execução da ferramenta de remoção. Isso também pode funcionar para outros firewalls, mas não foi confirmado.

O que a ferramenta faz

A ferramenta de remoção do W32.Blaster.Worm faz o seguinte:

1. Finaliza os processos virais do W32.Blaster.Worm.
2. Exclui os arquivos do W32.Blaster.Worm.
3. Exclui os arquivos gravados na máquina pelo worm.
4. Exclui os valores de Registro adicionados pelo vírus.

Parâmetros de linha de comando disponíveis para essa ferramenta

Parâmetro	Descrição
/HELP, /H, /?	Exibe a mensagem de ajuda.
/NOFIXREG	Desativa a correção do registro (o uso dessa opção não é recomendado)
/SILENT, /S	Habilita o modo silencioso.
/LOG=<caminho>	Cria um arquivo de registro onde <caminho> é o local para armazenar as saídas da ferramenta. Por padrão, será criado um arquivo de registro FixBlast.log na mesma pasta em que a ferramenta for executada.
/MAPPED	Verifica os discos de rede mapeados (o uso dessa opção não é recomendado -- veja Notas abaixo).
/START	Força a ferramenta a iniciar a verificação imediatamente.
/EXCLUDE=<caminho>	Exclui especificamente a pasta localizada no <caminho> da verificação (não recomendamos o uso dessa opção).

NOTA: O uso da opção /MAPPED não garante a total remoção do vírus no computador remoto, pois:

- A verificação dos discos mapeados é executada apenas nas pastas que foram mapeadas. Isto pode não incluir todas as pastas do computador remoto, levando a falhas na detecção.

- Se for detectado um arquivo infectado no disco mapeado, a remoção falhará se o computador remoto estiver usando esse arquivo. Por essas razões, você deve executar a ferramenta em cada um dos computadores.

Para obter e executar a ferramenta

NOTA: Você deve ter privilégios de administrador para executar essa ferramenta no Windows 2000/XP.

1. Faça o download do arquivo FixBlast.exe clicando no link abaixo:
   http://securityresponse.symantec.com/avcenter/FixBlast.exe

2. Salve o arquivo em um lugar conveniente, como a pasta de download, a área de trabalho do Windows ou numa mídia removível que não esteja infectada, se possível.

3. Para verificar a autenticidade da assinatura digital, veja a seção **Assinatura digital**.

4. Feche todos os programas antes de executar a ferramenta.

5. Se você estiver em rede ou tiver uma conexão permanente com a Internet, desconecte seu computador. Se você estiver usando Windows ME ou XP, desabilite a Restauração do Sistema.

6. Para mais detalhes, veja a seção **Opção de Restauração do Sistema no Windows ME ou XP**.

CUIDADO: Se você estiver usando o Windows ME/XP recomendamos enfaticamente que você não ignore esse passo. O processo de remoção poderá falhar se a Restauração do Sistema do Windows Me/XP não estiver desabilitada, porque o Windows não permite que outros programas modifiquem a Restauração do Sistema.

7. Clique duas vezes no arquivo FixBlast.exe para iniciar a ferramenta de remoção.

8. Clique em Start [Iniciar] para iniciar o processo e deixe a ferramenta ser executada.

   NOTA: Se, ao executar a ferramenta, aparecer uma mensagem de que a ferramenta não conseguiu excluir um ou mais arquivos infectados, você deverá executar a ferramenta em Modo de Segurança. Saia do Windows, desligue o computador no botão de força e aguarde durante 30 segundos. Reinicie o computador em Modo de Segurança e execute a ferramenta novamente. Todos os sistemas operacionais de 32-bits, com exceção do Windows NT, podem ser inicializados em Modo de Segurança. Para instruções sobre como fazer isso, consulte o documento Como iniciar o Windows 95/98/Me no Modo de Segurança.

9. Reinicie o computador.

10. Execute a ferramenta de remoção mais uma vez para assegurar-se de que o sistema esteja limpo.

11. Se estiver usando o Windows ME ou XP, habilite novamente a opção de Restauração do Sistema.

12. Execute o LiveUpdate para assegurar-se de estar com as definições de vírus mais atualizadas.

Quando a ferramenta terminar a execução, você verá uma mensagem informando se o computador estava infectado pelo W32.Blaster.Worm. No caso de remoção do worm, o programa mostra os seguintes resultados:

- O número total de arquivos verificados
- O número de arquivos apagados
- O número de processos virais terminados
- O número de entradas do registro apagadas

Assinatura Digital

O FixBlast.exe é assinado digitalmente. A Symantec recomenda que você use somente cópias do FixBlast.exe que tenham sido obtidas diretamente do site de download do Symantec Security Response. Para verificar a autenticidade da assinatura digital, siga esses passos:

1. Vá até http://www.wmsoftware.com/free.htm

2. Faça o download e salve o arquivo Chktrust.exe na mesma pasta em que você salvou o FixBlast.exe (por exemplo, C:\Downloads).

3. Dependendo do seu sistema operacional, faça o seguinte:
   - Clique em Iniciar, selecione Programas e clique em Prompt do MS-DOS.
   - Clique em Iniciar, selecione Programas, clique em
   - Acessórios e então, clique em Prompt do MS-DOS.

4. Mude para o diretório no qual o FixBlast.exe e Chktrust.exe foram salvos e digite:**chktrust -i FixBlast.exe**

   Por exemplo, se você salvou os arquivos na pasta C:\Downloads, deve digitar os seguintes comandos (pressione Enter após digitar cada comando)
   :cd\
   cd downloads
   chktrust -i FixBlast.exe

   Pressione Enter após ter digitado cada comando. Se a assinatura digital for válida, você será o seguinte: Do you want to install and run "W32.Blaster.Worm Removal Tool" signed on 8/11/2003 7:14 PM and distributed by Symantec Corporation?

   (Você deseja instalar e executar a "Ferramenta de Remoção do W32.Blaster.Worm" assinada em 11/8/2003 às 19h14m e distribuída pela Symantec Corporation?)

NOTAS:
- A data e a hora que aparecem na caixa de diálogo serão ajustadas para o seu fuso horário, se o seu computador não estiver configurado para a hora do Pacífico.
- Se estiver em Horário de Verão a hora exibida será exatamente uma hora mais cedo.
- Se essa caixa de diálogo não aparecer, há duas possíveis razões:

- Essa ferramenta não é da Symantec. A menos que tenha certeza de que a ferramenta seja legítima e que realmente tenha sido obtida através do site da Symantec, você não deve executá-la.
- A ferramenta é da Symantec e é legitima. Entretanto, seu sistema operacional foi previamente configurado para sempre confiar nos produtos da Symantec. Para informações sobre isto e sobre como ver novamente a caixa de confirmação, leia o documento How to restore the Publisher Authenticity confirmation dialog box (Este recurso encontra-se em inglês).

5. Clique Yes (Sim) para fechar a caixa de diálogo.
6. Digite Exit e pressione Enter. Isso fechará a sessão MS-DOS.

Opção Restauração do Sistema no Windows Me ou XP

Usuários do Windows Me e do Windows XP devem desabilitar temporariamente a Restauração do Sistema. Este recurso, habilitado por padrão, é usado pelo Windows ME/XP para restaurar os arquivos no seu computador, caso tenham sido danificados. Quando um computador é infectado por um vírus, worm ou Cavalo de Tróia é possível que essas ameaças sejam restauradas pela Restauração do Sistema.

O Windows previne que a Restauração do Sistema seja alterada por programas externos. Assim, programas antivírus ou ferramentas de remoção não conseguem remover limpar arquivos da pasta de Restauração do Sistema. Como resultado, o recurso possui potencial para infectar o computador novamente, caso uma restauração seja executada. Para instruções sobre como desligar a Restauração do Sistema, consulte a documentação do Windows ou um dos seguintes artigos:

- Como desativar ou ativar o recurso de restauração do sistema no Windows Me
- Como desativar ou ativar o recurso de restauração do sistema no Windows XP

Para informações adicionais, ou uma alternativa a desabilitação do recurso, consulte o documento da Base de Dados da Microsoft Antivirus Tools Cannot Clean Infected Files in the _Restore Folder (Q263455) (este recurso encontra-se em Inglês).

Como executar a ferramenta a partir um disquete

1. Insira o disquete que contém arquivo FixBlast.exe na unidade de disco flexível.

2. Clique no botão Iniciar e então, em Executar.

3. Digite o comando abaixo e clique no botão OK:

a:\FixBlast.exe

and then click OK.

NOTAS:
- Não há espaços no comando a:\FixBlast.exe
- Se você estiver usando o Windows ME e a Restauração do Sistema estiver habilitada, surgirá uma mensagem de alerta. Escolha entre executar a ferramenta de remoção com a opção Restauração do Sistema habilitada ou sair da ferramenta de remoção.

4. Clique Start (Iniciar) para começar o processo e deixe a ferramenta ser executada.