

**ESCOLA SUPERIOR ABERTA DO BRASIL - ESAB
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM
REDES DE COMPUTADORES**

PAULO RICARDO MATOS CÂMARA

**SEGURANÇA DOS DADOS NAS EMPRESAS:
PROBLEMAS E SOLUÇÕES**

**VILA VELHA - ES
2010**

PAULO RICARDO MATOS CÂMARA

**SEGURANÇA DOS DADOS NAS EMPRESAS:
PROBLEMAS E SOLUÇÕES**

Monografia apresentada ao Curso de Pós-Graduação em Redes de Computadores da Escola Superior Aberta do Brasil como requisito para obtenção do título de Especialista em Redes de Computadores, sob orientação do Prof. Marcos Alexandre do Amaral Ramos.

**VILA VELHA - ES
2010**

PAULO RICARDO MATOS CÂMARA

**SEGURANÇA DOS DADOS NAS EMPRESAS:
PROBLEMAS E SOLUÇÕES**

Monografia aprovada em ... de de 2010.

Banca Examinadora

**VILA VELHA - ES
2010**

Dedico este trabalho à minha mãe que sempre me apoiou nos momentos mais difíceis;

A meu pai que sempre me orientou e ajudou nos meus estudos;

AGRADECIMENTOS

Aos meus professores/tutores pela
presteza em responder minhas dúvidas;

Ao meu orientador Prof. Marcos
Alexandre do Amaral Ramos.

“Os verdadeiros analfabetos são aqueles
que aprenderam a ler e não lêem.”
(Mário Quintana)

RESUMO

Palavras-chave: Segurança; Empresas; Redes de computadores

Este trabalho faz uma breve explanação acerca dos problemas e soluções existentes atualmente relacionados à segurança dos dados nas redes de computadores nas corporações. Demonstramos a tendência atual das empresas em cada vez mais estarem automatizando seus processos de negócios e digitalizando seus dados, utilizando os mais diversos recursos tecnológicos e transformando-se de empresas tradicionais em empresas digitais. Diante dessa tendência, expomos as soluções existentes para evitar a perda de informações importantes e para prevenir a divulgação de dados confidenciais. Destacando a importância da preocupação com a segurança, descrevemos as principais vulnerabilidades e ameaças aos quais estão sujeitos os sistemas computacionais e apresentamos procedimentos e formas de minimizá-las. Apresentamos os principais ataques que podem ser realizados contra as redes de computadores cabeadas e sem fio, os tipos de atacantes e técnicas e ferramentas que podem evitá-los. Essa pesquisa também evidencia a importância do treinamento dos funcionários das empresas quanto às ameaças contra a segurança dos sistemas e a necessidade de conscientização de todos para cumprir os procedimentos determinados na política de segurança das organizações. Concluímos com a compreensão do quanto se tornou importante a preocupação com segurança dos dados nesse processo de transformação pelo qual as organizações passam atualmente. Quanto à metodologia utilizada, foram realizadas diversas pesquisas em livros, *Internet* e materiais relacionados ao assunto para atingir esses objetivos.

LISTA DE FIGURAS

Figura 1 – Fatores que levam à transformação das empresas tradicionais em digitais	13
Figura 2 – Rede de computadores de uma empresa ligada à <i>Internet</i>	14
Figura 3 – Como funciona o <i>RAID 0+1</i>	18
Figura 4 – <i>No-break</i> : para evitar danos a equipamentos	19
Figura 5 – Ferramenta “ <i>tracert</i> ” no <i>Windows</i>	36
Figura 6 – Uso do <i>firewall</i> para proteger uma <i>Intranet</i>	38
Figura 7 – Criptografia utilizando chaves	39
Figura 8 – A complexidade da rede de comunicações entre a matriz, filiais e parceiros de uma empresa	41
Figura 9 – Simplicidade nas ligações com a utilização de <i>VPNs</i>	42
Figura 10 – <i>Switch</i>	46
Figura 11 – Câmera de vídeo: pode ser usada para aumentar a segurança	47
Figura 12 – Planejamento da política de segurança	49
Figura 13 – Um atacante pode realizar um ataque mesmo no ambiente externo à empresa	54

SUMÁRIO

INTRODUÇÃO	10
CAPÍTULO 1 – AS EMPRESAS DIGITAIS E AS REDES DE COMPUTADORES	13
CAPÍTULO 2 – PREVENINDO PERDA DE DADOS POR DANOS OU FALHAS EM EQUIPAMENTOS	16
2.1 – RAID	16
2.2 – SALA COFRE	18
2.3 – <i>NO-BREAK</i>	19
CAPÍTULO 3 – TIPOS DE ATACANTES	21
3.1 – <i>HACKERS</i>	21
3.2 – <i>CRACKERS, BLACKHATS OU FULL FLEDGEDS</i>	21
3.3 – <i>SCRIPT KIDDIES</i>	22
3.4 – <i>INSIDERS</i>	22
3.5 – <i>CYBERPUNKS</i>	25
3.6 – <i>CODERS</i>	25
3.7 – <i>WHITE HATS</i>	26
3.8 – <i>GRAY HATS</i>	27
3.9 – <i>PHREAKERS</i>	27
3.10 – <i>CYBERTERRORISTAS</i>	27
CAPÍTULO 4 – TIPOS DE ATAQUES	29
4.1 – ENGENHARIA SOCIAL	29
4.2 – ATAQUE FÍSICO	30
4.3 – <i>PACKET SNIFFING</i>	30
4.4 – <i>DUMPSTER DIVING</i>	31
4.5 – INFORMAÇÕES LIVRES	32
4.6 – <i>PORT SCANNING</i>	33
4.7 – <i>SCANNING DE VULNERABILIDADES</i>	33
4.8 – <i>IP SPOOFING</i>	35
4.9 – ATAQUES DE NEGAÇÃO DE SERVIÇOS (<i>DENIAL OF SERVICE-DOS</i>)	35
4.10 – <i>FIREWALKING</i>	36
CAPÍTULO 5 – TÉCNICAS E FERRAMENTAS PARA DEFESA	38

5.1 – FIREWALL	38
5.2 – CRIPTOGRAFIA	39
5.3 – AUTENTICAÇÃO	40
5.4 – REDES PRIVADAS VIRTUAIS (VPNs)	40
5.5 – SISTEMAS DE DETECÇÃO DE INTRUSÃO	42
5.6 – DEFENDENDO-SE DE <i>SNIFFERS</i>	43
5.7 – DEFENDENDO-SE DE ATAQUES FÍSICOS	46
5.8 – POLÍTICA DE SEGURANÇA	48
CAPÍTULO 6 – PROBLEMAS DE SEGURANÇA EM REDES SEM FIO	50
6.1 – VULNERABILIDADES DOS PROTOCOLOS <i>WEP</i> E <i>WPA</i>	50
6.2 – CONFIGURAÇÕES DE FÁBRICA	51
6.3 – ACESSO NÃO PERMITIDO EM CONFIGURAÇÕES BÁSICAS	52
6.4 – ENVIO E RECEPÇÃO DE SINAL	53
6.5 – MAPEAMENTO DO AMBIENTE	54
6.6 – CAPTURA DE TRÁFEGO	54
6.7 – NEGAÇÃO DE SERVIÇO	55
6.8 – APARELHOS <i>WI-FI</i> EM REDES CABEADAS	55
6.9 – SEGURANÇA FÍSICA	56
CAPÍTULO 7 – TÉCNICAS DE DEFESA EM REDES SEM FIO	58
CAPÍTULO 8 – A IMPORTÂNCIA DO TREINAMENTO DOS FUNCIONÁRIOS DA ORGANIZAÇÃO	60
CONCLUSÃO	62
REFERÊNCIAS	64

INTRODUÇÃO

A globalização, a *Internet* e a nova Era do conhecimento têm proporcionado grandes mudanças no mundo corporativo. A integração das informações tanto internamente, entre os setores da empresa, quanto entre suas filiais, seus clientes e parceiros comerciais tornou-se um fator muito importante para assegurar o poder competitivo. A integração digital está mudando a maneira como as empresas são administradas, organizadas e a relação delas com seus clientes. Atualmente é impossível imaginar uma empresa desprezando o aspecto tecnológico em seus negócios.

Essas transformações estão fazendo surgir corporações totalmente digitais nas quais todas as transações com clientes e parceiros ocorrem digitalmente, assim como os dados que dão suporte às decisões empresariais devem estar disponíveis em qualquer parte da organização.

Ao mesmo tempo, esse compartilhamento e exposição de dados entre as diversas peças participantes do mundo empresarial trouxeram diversos problemas e vulnerabilidades. De um lado, a transmissão dos dados e as transações acontecem muito mais rapidamente e a concretização dos negócios é facilitada pela tecnologia da informação. Por outro lado essa facilidade que o mundo digital trouxe também veio acompanhada de preocupações relacionadas à segurança nas redes de computadores e perdas de informações nos computadores, entre outras.

Nesse processo de transformação, a quantidade de informações das empresas que deixam o papel e é armazenada em mídias digitais tem crescido muito. O que antes ficava restrito ao ambiente ou rede interna das corporações, hoje pode ser acessado de qualquer lugar do mundo através da *Internet*. Diante desse cenário, quais os problemas que surgem relacionados à segurança dos dados das empresas e o que fazer para evitá-los ou enfrentá-los? Esse trabalho de pesquisa tem o intuito de responder essa pergunta e apresentar os desdobramentos e implicações que surgem como consequência das mudanças pelas quais a sociedade passa com a popularização da *Internet* e digitalização das informações nas instituições.

O objetivo geral desse trabalho de pesquisa é Identificar os problemas e soluções relacionados à segurança dos dados nas corporações.

E especificamente, buscaremos atingir os seguintes objetivos:

- Demonstrar a tendência atual das Empresas Tradicionais ou Clássicas estarem se transformando em Empresas Digitais;
- Apresentar as vantagens e desvantagens que se manifestam com a diminuição do uso do papel e a digitalização das informações;
- Mostrar os problemas que surgem com a ligação das *intranets* ou redes internas das corporações à *Internet*;
- Identificar as soluções existentes para evitar a perda de dados e invasão das redes das instituições conectadas à *Internet*;
- Expor os benefícios e as vulnerabilidades que as redes sem fio (*wireless*) podem trazer para as organizações, assim como formas de diminuir a ocorrência de invasão a elas;
- Descrever os ataques que podem ocorrer às redes de computadores e meios de prevenir ou minimizar seus danos;
- Indicar formas de prevenir a perda de dados por falha de equipamentos nos servidores ou estações de trabalho;
- Explicar a importância do treinamento dos funcionários com relação à política de segurança da corporação.

As razões para escolha deste tema para a monografia se deram devido às minhas observações e preocupações quanto à segurança dos dados nas redes de computadores na instituição na qual trabalho. A maior utilização dos recursos tecnológicos e digitais pelas empresas traz problemas com a segurança dos dados, o que justifica a importância do estudo e da pesquisa nessa área para toda a sociedade.

No capítulo 1, falaremos sobre como está ocorrendo o processo de transformação da empresas tradicionais em digitais, com a diminuição do uso do papel, digitalização das informações, maior utilização das redes de computadores e ligação das *intranets* das organizações à *Internet*. Nos capítulos 2, demonstraremos

algumas medidas que podem ser tomadas para prevenir a perda de informações por falhas em equipamentos. Nos capítulos 3, 4 e 5, apresentaremos os tipos de atacantes, ataques e métodos ou ferramentas que podem ser utilizados para proteger as redes de computadores. Nos capítulos 6 e 7, mostraremos problemas de segurança relacionados às redes sem fio e maneiras de minimizá-los. E finalmente no capítulo 8 demonstraremos a importância do treinamento dos empregados das empresas para prevenir problemas de segurança de dados.

A realização do trabalho será feita através de pesquisa exploratória em livros, revistas e *Internet*. Serão identificados os problemas de segurança que as empresas podem enfrentar, assim como meios de contorná-los, através de pesquisa bibliográfica em materiais relacionados ao assunto.

CAPÍTULO 1 – AS EMPRESAS DIGITAIS E AS REDES DE COMPUTADORES

Com a crescente e rápida evolução da tecnologia na nossa sociedade, as empresas tradicionais, empresas clássicas que ainda usam o papel em todos os seus processos de negócios já não irão mais existir no futuro. A globalização, a era do conhecimento, a tecnologia da informação e a *Internet* estão entre os fatores que contribuem para essa mudança nas organizações. As corporações estão cada vez mais se utilizando dos sistemas de informações computacionais e interligando suas intranets à *Internet* para realizar seus negócios (VALENTE, 2007).

A importância dos sistemas de informações para o mundo dos negócios é destacada por LAUDON (2004, p. 6):

As empresas estão sempre tentando melhorar a eficiência de suas operações a fim de conseguir maior lucratividade. Das ferramentas de que os administradores dispõem, as tecnologias e os sistemas de informações estão entre as mais importantes para atingir altos níveis de eficiência e produtividade nas operações [...]

As empresas tradicionais, na tentativa de se adaptar a essas mudanças tecnológicas estão se transformando em empresas mistas, que seriam um estado de transição entre a tradicional e a digital. As empresas, primeiramente adaptam-se ao modelo de empresa mista e, depois, seguem na direção da digital. Na empresa digital, o papel seria praticamente extinto e todas as informações transitam digitalmente dentro da organização, entre seus parceiros e clientes (VALENTE, 2007).

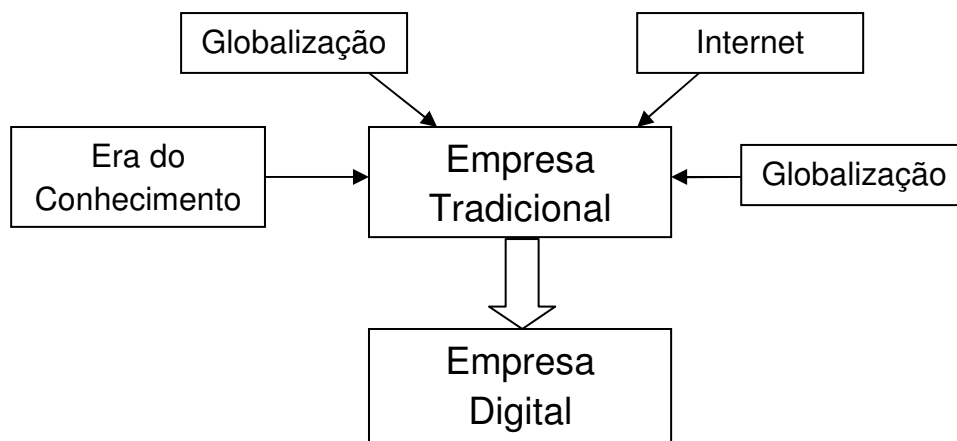


Figura 1 - Fatores que levam à transformação das empresas tradicionais em digitais
Fonte: Elaboração própria (2010)

A evolução da tecnologia da informação e a redução dos custos dos computadores tornaram a distribuição do poder computacional em módulos localizados em diversos pontos das organizações uma solução cada vez mais atraente para melhorar a eficiência e facilidade de acesso aos dados. E a necessidade do compartilhamento de recursos de *hardware* e *software* para permitir a troca de informações deu origem um espaço oportuno para o desenvolvimento dos sistemas de informações e das redes de computadores. A microeletrônica e a tecnologia de comunicações vêm evoluindo muito e como conseqüência, as redes de computadores estão cada vez mais presentes em nossas vidas. A União entre comunicação e processamento revolucionou o mundo em que vivemos, abrindo as portas para novas formas de comunicação e trazendo maior eficiência para os sistemas computacionais.

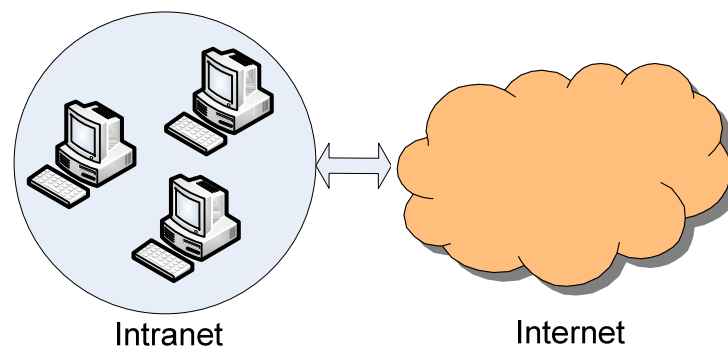


Figura 2 – Rede de computadores de uma empresa ligada à Internet
Fonte: Elaboração própria (2010)

Esse processo que envolve a diminuição ou extinção do papel, digitalização das informações e conexão das *intranets* das empresas à *Internet* proporciona diversas vantagens como apontam LAUDON (2004) e O'BRIEN (2004):

- Simplicidade na realização dos negócios;
- Rapidez na concretização de transações;
- Facilidade em se realizar pesquisas sobre os dados da organização, como sobre informações financeiras, por exemplo;
- Maior detalhamento de informações sobre clientes, funcionário, fornecedores, etc;
- Acesso rápido e instantâneo a informações de qualquer lugar do mundo, assim como a possibilidade de atualizá-los.

Porém, LAUDON (2004) e O'BRIEN (2004) mencionam que essas vantagens vêm acompanhadas de algumas desvantagens como:

- Aumentam os problemas relacionados à segurança dos dados;
- Indivíduos podem acessar e alterar informações da organização de qualquer lugar do mundo, causando grandes prejuízos;
- Crescem os gastos com tecnologia para minimizar problemas de segurança ou perda de dados;
- Necessidade de treinamento e conscientização de todos os funcionários quanto à importância da segurança das informações, acarretando mais gastos;

Devido também ao custo, tornou-se importante a conexão entre os sistemas para o compartilhamento de dispositivos periféricos como impressoras, por exemplo. Outro fator que também levou a esta interconexão foi a capacidade de troca de dados. Os usuários não trabalham isoladamente, precisavam se comunicar com outros setores da organização e de facilidade de acesso a informações e programas de várias fontes. Assim, ambientes cooperativos tornaram-se realidade reforçando ainda mais a necessidade da interconexão dos equipamentos nas instituições (TANENBAUM, 2003).

CAPÍTULO 2 – PREVENINDO A PERDA DE DADOS POR DANOS OU FALHAS EM EQUIPAMENTOS

Geralmente, a implantação da informática nas empresas ocorre de forma gradual. No início, apenas determinadas funções são automatizadas e depois, à medida que a informatização vai se estabelecendo, outras funções vão sendo colocadas no mundo digital. Nessas situações pode existir redundância de dados entre os setores, matriz e filiais, que ocasiona entradas repetidas da mesma informação e inconsistência entre os dados. A solução para evitar isso é o compartilhamento de informações, onde cada informação é armazenada uma única vez, sendo acessada pelos vários sistemas que dela necessitam (HEUSER, 2004).

Dessa forma, temos o conjunto de dados integrados da organização que vai atender à comunidade de usuários armazenada em um banco de dados localizado em um servidor. Apresentaremos a seguir ferramentas ou técnicas que podem ser utilizadas para prevenir a perda dessas informações tão importantes nos servidores das empresas e até nas estações de trabalho dos funcionários.

2.1 – RAID

Possuir um maior número de discos rígidos pode melhorar o desempenho e a confiabilidade do armazenamento de dados em um sistema, como afirma KORTH (2006, p.300):

Ter um grande número de discos em um sistema dá a oportunidade de melhorar a taxa na qual os dados são lidos ou escritos, se os discos são operados em paralelo. Adicionalmente, essa configuração oferece o potencial de melhorar a confiabilidade do armazenamento de dados, porque informações redundantes podem ser armazenadas em diferentes discos.

Dessa forma, a falha em um disco não acarretará perda de dados. Diversas técnicas de organização de discos comumente chamadas de *RAID* (*redundant array of independent drives*) existem para prevenir a perda de informações importantes nas empresas. Assim, a solução para o problema da confiabilidade é introduzir

redundância, ou seja, armazenar dados adicionais que não são normalmente necessários, mas que podem ser usados, se ocorrer a falha de um disco, para reconstruir o que foi perdido.

Segundo KORTH (2006), o método mais simples, porém mais caro, de introduzir redundâncias é duplicar cada disco. No espelhamento, como é chamada essa técnica, um disco lógico é formado por dois discos físicos e cada operação de escrita é realizada nos dois discos. Caso um dos discos físicos falhe, as informações podem ser lidas do outro. Só haverá perda de dados se o segundo disco falhar antes do primeiro que falhou ser reparado.

O espelhamento oferece alta confiabilidade, mas é caro, como foi dito. Vários esquemas têm sido propostos para oferecer redundância a baixo custo usando o modelo de espelhamento juntamente com a “paridade” de *bits*. Essas técnicas têm diferentes relações entre custo e desempenho e são classificadas em níveis chamados de níveis *RAID* (KORTH, 2006):

- *RAID* nível 0: é um arranjo de discos com distribuição paralela das informações. As informações são divididas em pequenas partes e distribuídas entre os discos, mas sem qualquer redundância. Por isso, caso ocorra falha em um dos discos pode ocorrer perda de dados. É utilizado para melhorar o desempenho do sistema;
- *RAID* nível 1: funciona como o espelhamento de disco discutido anteriormente, onde discos adicionais são instalados no computador e funcionam como cópias dos já existentes. Assim, se um disco principal falha, outro pode assumir as operações e continuar a disponibilizar informações;
- *RAID* nível 2: semelhante ao *RAID* 0, mas utiliza um esquema de detecção de erros por meio de bits de paridade;
- *RAID* nível 3: usa um disco rígido adicional para armazenar informações de paridade, aumentando ainda mais a confiabilidade dos dados armazenados;
- *RAID* nível 4: armazena blocos da mesma maneira que em discos comuns, sem redistribuí-los pelos discos, porém mantendo um bloco de paridade em um disco separado para os blocos correspondentes dos outros discos;

- *RAID* nível 5: melhora o *RAID* nível 4 através do distribuição de dados e paridade entre todos os N+1 discos, ao invés de armazenar as informações em N discos e a paridade em um único disco;
- *RAID* nível 6: é muito parecido com o *RAID* 5, mas armazena informações redundantes extras para prevenir falhas múltiplas de discos.
- *RAID* 0+1: combinação dos níveis 0 e 1, onde os dados são distribuídos entre os discos para melhorar o desempenho, mas também utiliza outros discos que mantêm cópias das informações.

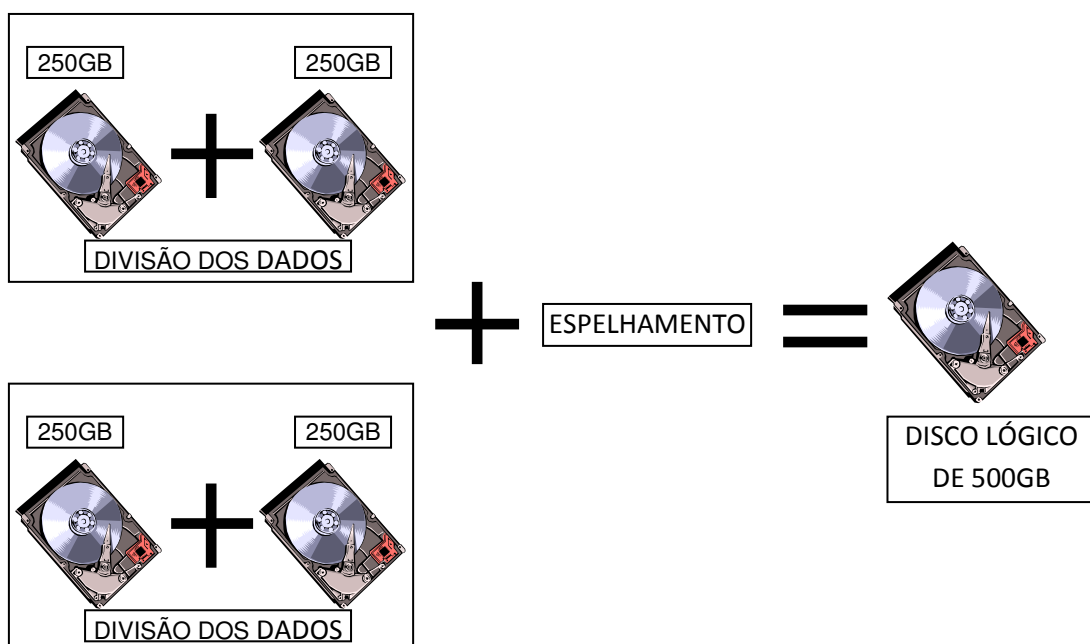


Figura 3 – Como funciona o RAID 0+1
 Fonte: Elaboração própria (2010)

2.2 – SALA COFRE

Uma sala-cofre é um ambiente projetado com os mais avançados recursos para proteger fisicamente os equipamentos mais importantes de uma organização como servidores de banco de dados ou equipamentos de comunicação essenciais ao funcionamento da empresa. É utilizada para proteger itens de alta importância operacional ou estratégica, cujas perdas possam ser significativas, de difícil recuperação e causar paralisação dos processos de negócios e um grande prejuízo.

São ambientes fabricados para suportar vários tipos de catástrofes inundações, terremotos, incêndios, terremotos, e outros (FERREIRA, 2008).

2.3 – NO-BREAK

No-breaks tornaram-se equipamentos muito importantes para diminuir os problemas com falhas nos equipamentos importantes das empresas. O *no-break* é o equipamento mais indicado para oferecer energia elétrica estabilizada, senoidal e sem interrupção para os componentes mais críticos da organização, prevenindo falhas e perda de dados (ENERGYBRAZ, 2010).

Nos servidores de banco de dados, as falhas de energia provavelmente não trarão problemas se uma transferência de dados para os discos não estiver em andamento quando acontecerem. No entanto, mesmo no caso de espelhamento de discos, se transações de escrita estiverem sendo feitas no mesmo bloco em ambos os discos, e acontecer uma falha de energia antes que as operações de escrita dos blocos sejam finalizadas, então os dois blocos podem ficar inconsistentes (KORTH, 2006).



Figura 4 – *No-break*: para evitar danos a equipamentos
Fonte: Elaboração própria (2010)

Antigamente, falhas de energia elétrica não produziam tantos prejuízos aos negócios das organizações, pois era pequena a quantidade de equipamentos usados que dependiam de eletricidade. O maior problema enfrentado nos dias de hoje são os surtos momentâneos ou os ruídos ocasionados pelo desligamento e religamento de equipamentos no sistema. Esses surtos, ruídos e interrupções na energia elétrica ocorrem todo o tempo e não podem ser percebidos pelas pessoas, porque acontecem na faixa de milésimos de segundo. Apesar de serem imperceptíveis aos humanos, podem prejudicar a produtividade das empresas e a vida dos usuários que adquirem cada vez mais aparelhos que dependem da eletricidade (ENERGYBRAZ, 2010).

CAPÍTULO 3 – TIPOS DE ATACANTES

O termo geral para identificar quem realiza um ataque a um sistema de computação é *hacker*. Entretanto, essa generalização tem várias ramificações, pois os ataques possuem objetivos diferentes, seu êxito depende do grau de segurança da rede e da capacidade do invasor. Segundo TANENBAUM (2003, p. 543):

A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém. [...] Para tornar uma rede segura, com frequência é necessário lidar com adversários inteligentes, dedicados e, às vezes, muito bem subsidiados.

A seguir, apresentamos uma classificação dos diversos tipos de atacantes.

3.1 – *HACKERS*

São especialistas em segurança e auditoria em sistemas de computação, que, através de algumas técnicas estudadas e outras próprias, procuram falhas nesses sistemas. Ou ainda, utilizam o conhecimento que possuem para invadir sistemas, não com a intenção de causar danos às vítimas, mas como uma forma de desafio às suas habilidades. Podem invadir redes de computadores ou sistemas, acessar ou alterar arquivos para provar o quanto são capazes de realizar essas ações e para, depois, mostrar suas façanhas para os companheiros. Não querem prejudicar, mas somente provar quanto conhecimento e poder possuem. Os *hackers* não gostam de ser confundidos com os *crackers*, são excelentes programadores e conhecem muito bem os segredos das redes e dos computadores (OLIVEIRA, 2008).

3.2 – *CRACKERS, BLACKHATS OU FULL FLEDGEDS*

São indivíduos que invadem sistemas para subtrair informações indevidamente e produzir danos às vítimas. Além disso, decifram códigos e destroem proteções de programas de computador. São os verdadeiros terroristas da Internet e, sem medir

as conseqüências de seus atos, fazem o que for preciso para conseguir o que querem. Os *crackers* são, até mesmo, desprezados pelos próprios *hackers*. Às vezes, tentam vender as informações roubadas para a própria vítima, ameaçando torná-las públicas se a empresa ou usuário não pagar o valor pedido por eles (OLIVEIRA, 2008).

3.3 – *SCRIPT KIDDIES*

OLIVEIRA (2008) afirma que são principiantes e inexperientes, mas podem acarretar diversos problemas para as corporações. Também são chamados de *newbies*. Geralmente buscam informações e ferramentas encontradas prontas na Internet e as utilizam sem saber o que estão fazendo. Essas ferramentas são bem fáceis de ser obtidas, por isso os *newbies* podem trazer perigo a um grande quantidade de empresas, principalmente as que não possuem uma política de segurança definida adequadamente.

As corporações que não têm uma política de segurança conveniente sempre apresentam “brechas” de segurança em seus sistemas que podem ser exploradas por esses indivíduos, como as causadas pela não realização de atualização dos sistemas operacionais ou softwares, por exemplo. Os *script kiddies* são a grande maioria dos elementos que tentam invadir sistemas na Internet, assim há uma grande quantidade de problemas que são causados por eles. A difusão da Internet nos últimos tempos ajudou na disseminação dos *newbies* fazendo com que se transformassem nos maiores responsáveis pelo começo do processo de conscientização das corporações, que começaram a se interessar mais pelos problemas de segurança.

3.4 – *INSIDERS*

Segundo OLIVEIRA (2008), são pessoas que trabalham dentro da própria organização. São considerados os causadores dos incidentes de segurança mais

graves. Pesquisas demonstram que o número de ataques que tem como origem a Internet é maior que os ataques internos, mas os prejuízos maiores ainda são causados pelos últimos. Dessa forma, deve ser dada muita importância aos ataques cuja origem está na própria rede interna, realizados por indivíduos que conseguem infiltrarem-se na corporação, funcionários ou ex-funcionários. Muitas questões estão relacionadas a esse processo como a relação entre funcionários e chefes, engenharia social, suborno e espionagem industrial. Assim como os cartéis de drogas e as máfias, a espionagem industrial, freqüentemente atribuída aos *insiders*, já é considerada uma nova forma de ação do crime organizado.

Os próprios funcionários das empresas são considerados as maiores ameaças como afirma MITNICK (2003, p. 130):

A grande maioria dos empregados que são transferidos, demitidos ou rebaixados nunca causa problemas. Mesmo assim é preciso apenas um deles para fazer uma empresa perceber tarde demais as medidas que poderiam ser tomadas para evitar o desastre. A experiência e as estatísticas têm mostrado claramente que a maior ameaça para a empresa vem de dentro. São as pessoas que estão dentro que têm um conhecimento grande do lugar onde ficam as informações valiosas e de onde a empresa pode ser atingida para causar o maior dano.

Eles têm a liberdade e o tempo que necessitam para procurar alguma informação de seus interesses nas mesas das outras pessoas. Podem ler e copiar documentos confidenciais e aproveitar-se da amizade dos colegas para roubar uma grande quantidade de dados que podem valer milhões, copiando-as para um simples *pen-drive*, por exemplo. O que mais ajuda a ação destes indivíduos é o fato deles conhecerem a cultura, as operações e os detalhes da corporação, tornando a espionagem muito mais fácil. Assim eles sabem quem são os concorrentes, onde são guardados os segredos e, principalmente, como eliminar os rastros do processo de espionagem. Isso torna difícil identificar essas pessoas e puni-las.

Mas apesar da dificuldade em se identificar os *insiders*, eles freqüentemente são funcionários descontentes com a empresa e acham que suas atividades não são reconhecidas pelos chefes. Muitas vezes, são destratados e querem mostrar seu valor fazendo algo que façam sentirem-se importantes. Os concorrentes podem

facilmente manipular esses indivíduos, persuadindo-os e sabendo que não se encontram em uma condição muito confortável dentro da empresa.

Há também aquele que está à procura de alguma atividade excitante que modifique sua rotina de trabalho. As organizações devem prestar bastante atenção aos *insiders*, pois podem estar perdendo mercado e espaço para seus concorrentes sem saber por que isso está acontecendo. Os concorrentes podem ter conseguido acesso a dados através do roubo de informações causados pelos *insiders*.

Os ex-funcionários são, grande parte das vezes, os indivíduos mais perigosos e deve-se ter um cuidado importante com eles. Ao ser demitido, eles podem querer vingança. Se saírem da corporação com tranqüilidade, podem querer apresentar seus conhecimentos ao chefe de outra empresa que porventura venha a contratá-los. Essa última pode até mesmo ser uma concorrente da empresa para a qual ele trabalhava anteriormente.

Outro risco pode ser os funcionários terceirizados. Eles podem não ter acesso a informações confidenciais, mas podem estudar e saber sobre os processos, pontos fracos e hábitos da corporação, podendo explorá-los no momento oportuno. Os funcionários terceirizados podem aceitar subornos para realizar a divulgação de dados confidenciais ou até mesmo subornar os próprios funcionários da empresa para conseguir acesso a segredos industriais.

É importante haver controle sobre o pessoal responsável pela segurança e limpeza pois, muitas vezes, essas pessoas têm acesso sem restrição a locais importantes onde podem estar guardados equipamentos e informações de essenciais. Como esses locais devem ser limpos por alguém, a engenharia social pode ser usada para se conseguir o ingresso a áreas restritas.

A segurança é, antes de tudo, um problema social e não apenas um problema tecnológico. Dessa forma, as organizações não podem esquecer os aspectos humanos, pessoais e sociais no processo de elaboração da estratégia de segurança (OLIVEIRA, 2008).

3.5 – *CYBERPUNKS*

De acordo com OLIVEIRA (2008), dedicam-se a invadir sistemas apenas pelo desafio ou por simples divertimento. A grande preocupação deles é com o governo que pode estar acessando dados privados das pessoas. Têm muito conhecimento e obsessão pela privacidade de suas informações, fazendo com que todas as suas comunicações sejam realizadas com criptografia. Muitas vezes, são os *cyberpunks* que acham vulnerabilidades em sistemas, serviços ou protocolos, fazendo um grande favor às corporações, divulgando as falhas encontradas. Isso contribui para que os fabricantes de softwares corrijam seus programas e passem a desenvolvê-los dando maior importância à segurança. Entretanto, os fabricantes de programas ainda têm preferência por corrigir seus programas a escolher um método de desenvolvimento dos *softwares* com mais enfoque na segurança. Isso pode ser constatado através do grande número de falhas que ainda aparecem nos sistemas.

3.6 – *CODERS*

OLIVEIRA (2008) afirma que são indivíduos que decidiram realizar o compartilhamento de seus conhecimentos escrevendo livros, ministrando cursos, através de palestras e seminários, por exemplo, para relatar suas façanhas. Um desses casos é o de Kevin Mitnick. Depois de cumprir pena prisional por suas ações envolvendo engenharia social e aplicação de técnicas para acessar dados confidenciais de várias organizações, ele tornou-se muito solicitado para proferir palestras sobre segurança da informação. Mas teve que conseguir uma aprovação formal para isso, pois não tinha permissão de usar computadores, trabalhar como consultor na área de tecnologia da informação e escrever sobre tecnologia sem a uma autorização. Somente no ano de 2001, ele teve restabelecido o direito de usar um telefone celular e começou a trabalhar em um seriado de televisão, onde fazia o papel de um especialista em computação membro da *CIA*. Hoje, depois de vencer o período de observação, ele criou uma empresa de consultoria e já escreveu livros muito famosos como “A arte de enganar”, por exemplo.

3.7 – WHITE HATS

OLIVEIRA (2008) afirma que os *white hats* usam suas habilidades para encontrar falhas de segurança nos sistemas e realizar as correções necessárias, trabalhando profissionalmente e legalmente nas empresas. Também são conhecidos como “*hackers do bem*”, “*hackers éticos*”, samurais ou *sneakers*. São tidos como guerreiros que tem a função de proteger os sistemas de computação das corporações e, para isso, realizam testes de invasões, simulam ataques para verificar o nível de segurança da rede e efetuam diversas análises necessárias para proteger os dados das empresas.

Porém, deve-se tomar uma série de cuidados antes de contratar os serviços de um *white hat*. É preciso determinar limites na simulação de ataques para prevenir uma exposição de dados confidenciais. Outro ponto importante é colocar de forma clara no contrato que os dados obtidos permanecerão sob sigilo e a garantia se que as correções necessárias devem ser executadas. Um *white hat* pode ser importante para a segurança de uma empresa, mas limites precisam ser impostos para que uma situação indesejada não ocorra no futuro. Eles podem achar diversas vulnerabilidades no sistema e depois querer cobrar para efetuar as correções necessárias.

Quando novas funcionalidades vão sendo implementadas no ambiente computacional da organização, sempre vão surgindo novas brechas de segurança e torna-se imprescindível a realização de novas análises de segurança. Isso termina trazendo mais custos. Manter um administrador responsável pela segurança dentro da corporação parece ser a solução mais adequada, pois a detecção desses problemas é um processo contínuo. Entretanto, se o administrador de segurança interno não possuir as habilidades necessárias para avaliar corretamente o nível de segurança dos sistemas, essa abordagem pode causar uma falsa impressão quanto às falhas do ambiente computacional.

A segurança é um aspecto multidisciplinar que abrange diversos fatores diferentes e caso as pessoas não possuam o conhecimento necessário sobre os riscos a que estão expostas, podem achar que estão seguras. Ou seja, não há como proteger-se contra o que não se conhece. Isso torna o conhecimento importantíssimo para uma proteção apropriada (MITNICK, 2003)

3.8 – GRAY HATS

De acordo com OLIVEIRA (2008), são *blackhats* trabalhando na área de segurança fazendo o papel de *whitehats*. Muitas empresas contratam-os para fazer análises de segurança, mas vários problemas já aconteceram e mostraram que o nível de confiança necessário para a execução dessas atividades tão críticas e estratégicas não é atingida através da contratação do serviço dessas pessoas.

A verdade é que utilizar os serviços de um *grayhat* para cuidar da segurança de uma instituição pode ser extremamente perigoso, principalmente por causa da própria natureza desses indivíduos. A publicação dos resultados de análises de segurança realizados em bancos por um *grayhat* foi um exemplo disso.

3.9 – PHREAKERS

Possuem grandes conhecimentos sobre informática e telefonia (OLIVEIRA, 2008). Podem invadir sistemas com o objetivo de espionar ligações alheias ou fazer ligações gratuitas.

3.9 – CYBERTERRORISTAS

OLIVEIRA (2008) afirma que seus ataques são contra alvos selecionados com cuidado e têm a intenção de divulgar mensagens religiosas ou políticas, danificar a estrutura de comunicações ou conseguir informações para comprometer a

segurança de algum país. Realizam pichações em sites, alterando uma página do site para difundir informações falsas e mensagens religiosas ou políticas, além de ataques de negação de serviços distribuídos e ataques a sistemas para conseguir dados confidenciais.

Numa época de guerras, como a dos Estados Unidos contra o Iraque e Afeganistão, deve-se ter bastante atenção a esses tipos de ataques. As invasões que produzem vazamentos de dados confidenciais podem acarretar graves conseqüências, ainda mais se envolverem a segurança nacional de um país. As ações de terroristas têm uma conexão crescente com o *cyberterrorismo* e é preocupante como a tecnologia e técnicas avançadas de ataque podem ser usadas juntamente com ações físicas de atos terroristas. Os terroristas podem usar estenografia e criptografia para o planejamento de ações, armazenamento de instruções e envio de mensagens (NAKAMURA, 2003).

CAPÍTULO 4 – TIPOS DE ATAQUES

4.1 – ENGENHARIA SOCIAL

É um procedimento que tenta tirar proveito das fraquezas humanas e sociais ao invés de explorar a tecnologia. A engenharia social busca iludir e enganar as pessoas utilizando-se de uma identidade falsa, para que elas revelem senhas ou outros dados importantes que venham a comprometer a segurança da empresa. Ela explora o fato dos funcionários estarem sempre prontos a colaborar e ajudar nos processos da empresa. Pode-se persuadir um indivíduo que está do outro lado de uma porta a abri-la independente do tamanho do cadeado. O utilizador dessa técnica manipula as pessoas para que forneçam senhas ou informações essenciais da instituição, explorando características importantes do seres humanos como, por exemplo, autoridade, medo, simpatia, busca por aprovação social, consistência e reciprocidade. Fazer-se passar por um alto funcionário com problemas urgentes para acessar o sistema é um caso clássico da utilização da engenharia social. O atacante transforma-se em um ator e, representando seu papel, explora a parte mais vulnerável da corporação: os seres humanos. Não é fácil identificar esse tipo de ataque, pois ele se utiliza de fatores como psicologia, confiança e a manipulação das pessoas. Um dos *hackers* mais famosos, Kevin Mitnick, usava a engenharia social em mais de 80% dos seus ataques (MITNICK, 2003).

O engenheiro social é considerado uma grande ameaça como aponta MITNICK (2003, p. 4):

Qual é a maior ameaça à segurança dos bens da sua empresa? Isso é fácil: o engenheiro social, um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos. Esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado.

Um dos procedimentos utilizados na engenharia social é visitar escritórios e distrair a secretária para que o invasor analise documentos que podem estar no computador ou em cima da mesa. Outra técnica usada é entrar pela porta dos fundos ou

garagem para acessar salas restritas ou até mesmo, disfarçar-se de entregador de flores ou pizzas. Apesar de requerer um espaço de tempo maior para conclusão, a criação de softwares com *bugs* inseridos propositalmente também é utilizado como forma de ataque na engenharia social. O atacante entrega esse programa na empresa para que faça testes com ele, pedindo que avisem a ocorrência de falhas e mostrando-se pronto a corrigi-las. A vítima poderia contatar o atacante que teria acesso a um computador da empresa para corrigir a falha que ele próprio introduziu, além de conseguir executar procedimentos relativos ao ataque em si como instalação de bombas lógicas ou *backdoors* (MITNICK, 2003).

4.2 – ATAQUE FÍSICO

De acordo com OLIVEIRA (2008), é o método de ataque que consiste no roubo de equipamentos, softwares ou mídias de armazenamento. Nessa técnica a realização do ataque dá-se diretamente no sistema, facilitando as ações por que não é necessário executar procedimentos remotos. Ao acessar o sistema diretamente, além do furto de equipamentos, pode-se efetuar vários atos destrutivos e maliciosos como ler e-mails de outras pessoas, fazer cópias de documentos confidenciais, alterar dados importantes, implantar armadilhas lógicas, modificar configurações, aumentar privilégios de usuários e obter informações privilegiadas como os salários dos funcionários e estratégia de novos produtos. A intenção e a imaginação do atacante é que vão servir de limite aos seus atos no sistema de forma que ele, obtendo o acesso físico, pode destruir todos os dados se essa for sua vontade.

A característica importante dos ataques físicos é o acesso direto ao sistema o que pode resultar em conseqüências de grandes proporções.

4.3 – *PACKET SNIFFING*

Esse procedimento se baseia na captura de dados importantes que transitam pela rede de computadores. É possível encontrar diversos programas que realizam essa

tarefa como, por exemplo, o *tcpdump*, fornecido junto com o *linux* e que, a princípio, seria utilizado para ajudar na solução de problemas relacionados à rede.

Softwares chamados *sniffers* podem capturar informações dos pacotes que trafegam no mesmo segmento de rede no qual o programa está sendo executado. É possível utilizar filtros para reter pacotes de protocolos específicos relativos a endereços *IP*, conteúdos e serviços. Em serviços de *e-mail*, *FTP* e *Telnet*, as senhas transitam abertamente pela rede e podem ser capturadas com bastante facilidade.

Para diminuir os problemas de segurança relacionados a essa técnica pode-se dividir a rede em diversos segmentos através da utilização de roteadores e *switches*. Mas em relação aos *switches*, essa providência não elimina totalmente a possível captura de pacotes no mesmo segmento onde o *sniffer* está sendo executado. Uma solução mais eficaz é o uso de protocolos que utilizam criptografia como o *IPSec* e o *SSH*. Também é necessário o uso de criptografia nos dados confidenciais que se movimentam pela rede, como em e-mails, para evitar a perda de sigilo (NAKAMURA, 2003).

4.4 – DUMPSTER DIVING

Também chamado de *trashing*, é o ato de procurar, no lixo, informações sobre a empresa, como nomes de contas, senhas, dados pessoais e informações confidenciais. Esse procedimento é eficiente e muito utilizado.

O lixo pode ser um tesouro para um atacante, como afirma MITNICK (2003, p. 128):

O seu lixo pode ser o tesouro do seu inimigo. Não damos muita atenção para os materiais que descartamos em nossa vida pessoal e, assim, por que acreditaríamos que as pessoas têm uma atitude diferente no local de trabalho? Tudo se resume a educar a força de trabalho sobre o perigo (as pessoas inescrupulosas que vasculham informações valiosas) e a vulnerabilidade (as informações confidenciais que não estão sendo destruídas ou apagadas adequadamente).

Uma propriedade interessante desse procedimento é o fato dele ser legal, pois os dados são colhidos direto do lixo. Casos de utilização dessa técnica são conhecidos

envolvendo bancos, nos quais o lixo dessas instituições foi verificado, na tentativa de encontrar dados importantes que foram estudados e cruzados com outras informações de clientes, resultando no acesso às contas dessas pessoas. Certos tipos de dados que, às vezes, não é dada grande importância são usados no plano de ataque como, por exemplo: inventários de hardware, fitas, formulários internos, disquetes, código fonte de programas, dados confidenciais impressos, manuais de sistemas de eventos e férias, calendário de reuniões, manuais de política de segurança, memorandos, organograma, lista telefônica, etc.

Dessa forma, um fragmentador de papel pode ser um acessório importante na política de segurança da organização para que os papéis sejam destruídos antes de ser enviados para o lixo (OLIVEIRA, 2008).

4.5 – INFORMAÇÕES LIVRES

Para iniciar um ataque, muitas informações podem ser adquiridas livremente na própria Internet, por exemplo. Não podem ser detectadas e alarmadas, sendo considerada não invasiva, a busca por informações livres incluem análise de cabeçalhos de e-mails, consultas a servidores *DNS* e acesso a dados em listas de discussão. Através delas, tem-se acesso facilmente a detalhes sobre a topologia da rede, usuários e sistemas. Mecanismos de busca como o *Yahoo* ou *Google* são bastante utilizados para se obter esses dados importantes, que torna-se mais fácil pela utilização de filtros.

Alguns protocolos podem ser usados para obtenção de informações como o *Simple Network Management Protocol (SNMP)* e o *NetBios*, além de serviços como *systat*, *netstat* e *finger*. Informações de protocolos como o *FTP* e *Telnet* que aparecem após a conexão do usuário ao serviço também podem mostrar a versão do serviço ou o tipo de sistema operacional, de forma que importante alterar essas configurações.

Cargos, funções de funcionários, números de telefones e outros dados interessantes podem ser encontrados em redes sociais e listas de discussão, por exemplo.

Também há a possibilidade do envio e-mails internos a listas de discussão desnecessariamente (OLIVEIRA, 2008).

4.6 – *PORT SCANNING*

São ferramentas usadas para se obter informações relacionadas aos serviços permitidos e definidos através do mapeamento das portas *UDP* e *TCP*. O *port scanning* fornece informações que permite evitar o desperdício de energia com ataques a serviços que não existem, podendo o atacante concentrar-se em técnicas que exploram serviços específicos que podem realmente ser atacados.

Um dos *port scanners* mais usados é o *nmap*. Ele também pode ser aproveitado para realização de auditoria no firewall e no *IDS* (Sistema de detecção de intrusão), assim como para determinar se o sistema tem falhas de implementação no protocolo *TCP/IP*, que podem ser exploradas em ataques do tipo negação de serviço. Além de mapear portas abertas, ele pode descobrir também, o sistema operacional da vítima e identificar qual usuário está executando cada serviço relativo a uma determinada porta (NAKAMURA, 2003).

4.7 – *SCANNING DE VULNERABILIDADES*

Depois de mapear o que pode ser atacado e os serviços em execução, as falhas específicas de cada sistema ou serviço podem ser descobertas através do *scanning* de vulnerabilidades. Eles executam vários testes na rede, procurando vulnerabilidades em aplicativos, serviços, protocolos e sistemas operacionais.

O mapeamento por uma ferramenta de *port scanning* torna-se importante, pois há a identificação prévia dos alvos, sistemas e serviços que podem ser atacados e o *scanning* de vulnerabilidades pode ser feito somente com o que foi mapeado. Evita-se, por exemplo, que falhas relativas apenas ao sistema operacional *windows* sejam verificadas em um computador com *linux*, o que seria desperdício de tempo e

esforço. Esses scanners podem examinar, através da análise de sistemas operacionais, checagem de roteadores, servidores, *firewalls* e outros elementos, os seguintes riscos: software desatualizado, configuração incorreta, compartilhamento de arquivos não protegidos por senhas, pacotes *TCP* que podem ter números de seqüência adivinhados, falhas no nível de rede de protocolos, *buffers overflows* em aplicativos, serviços e sistemas operacionais, evidência de falta de higiene em servidores web, configurações de roteadores perigosas, checagem de cavalos de tróia e senhas fáceis de adivinhar, configurações de serviços, possibilidade de negação de serviço, *SNMP* e configuração da política dos navegadores (NAKAMURA, 2003).

Assim, os *scanners* de vulnerabilidades podem ser também um meio para analisar riscos e para auditoria da política de segurança. São importantes, pois podem ser usados para mostrar os problemas de segurança da empresa, alertando os funcionários para a necessidade de analisar melhor os procedimentos de proteção às informações da corporação. Também são ferramentas bastante utilizadas por consultorias para demonstrar a necessidade de uma proteção melhor para, dessa maneira, vender seus serviços, tirando proveito da capacidade dos scanners de gerar relatórios para efetuar a avaliação técnica das falhas encontradas.

Entretanto, o conteúdo dos relatórios emitidos precisa ser conferido individualmente para evitar a ocorrência de falsos positivos e negativos. Uma falha relatada pode não corresponder à realidade do sistema ou alguma outra falha pode deixar de ser informada, devido ao fato da ferramenta trabalhar analisando uma base de dados com ataques conhecidos. Daí a necessidade de mantê-la sempre atualizada com as assinaturas de novos ataques.

O trabalho de análise feito por um profissional de segurança torna-se cada vez mais importante quando o número de novas vulnerabilidades cresce com muita velocidade. É fundamental que o cenário refletido seja o mais próximo do real para que não ocorra um alarme maior que o necessário ou uma falsa sensação de segurança, trazendo problemas para a empresa (NAKAMURA, 2003).

É importante salientar que essas ferramentas ajudam os administradores a proteger as redes, mostrando falhas a serem solucionadas, mas também são usadas por atacantes para detectar vulnerabilidades a serem exploradas. A utilização de sistemas de detecção de intrusão é uma boa medida preventiva que efetua a identificação de padrões de scanners e avisa o administrador de segurança o ocorrido (NAKAMURA, 2003).

4.8 – IP SPOOFING

Nesse método, o endereço verdadeiro do atacante é mascarado para evitar que ele seja encontrado. É bastante usada na tentativa de acessar sistemas cuja autenticação baseia-se em endereços *IP* e em ataques do tipo negação de serviço, onde pacotes de respostas não são necessários. Como esses pacotes são endereçados para o endereço *IP* falsificado, e não para o endereço real do atacante, o *IP spoofing* não permite que as respostas sejam obtidas. Para que um ataque tenha sua origem mascarada e as mensagens de resposta possam ser obtidas pelo atacante, é necessária a implementação de outras técnicas conjuntamente, como ataques de negação de serviço ao endereço *IP* da vítima forjada e mudança nas rotas das mensagens. Para proteger a rede de uma empresa do *IP spoofing* de endereços *IP* da rede interna, pode-se fazer uso de filtros de acordo com as interfaces de rede. Caso a rede de uma corporação tenha endereços do tipo 10.10.20.0, por exemplo, o *firewall* precisa bloquear tentativas de conexão de origem externa, nas quais a origem tem endereços de rede na faixa 10.10.20.0 (BURGESS, 2006).

4.9 – ATAQUES DE NEGAÇÃO DE SERVIÇOS (DENIAL OF SERVICE-DOS)

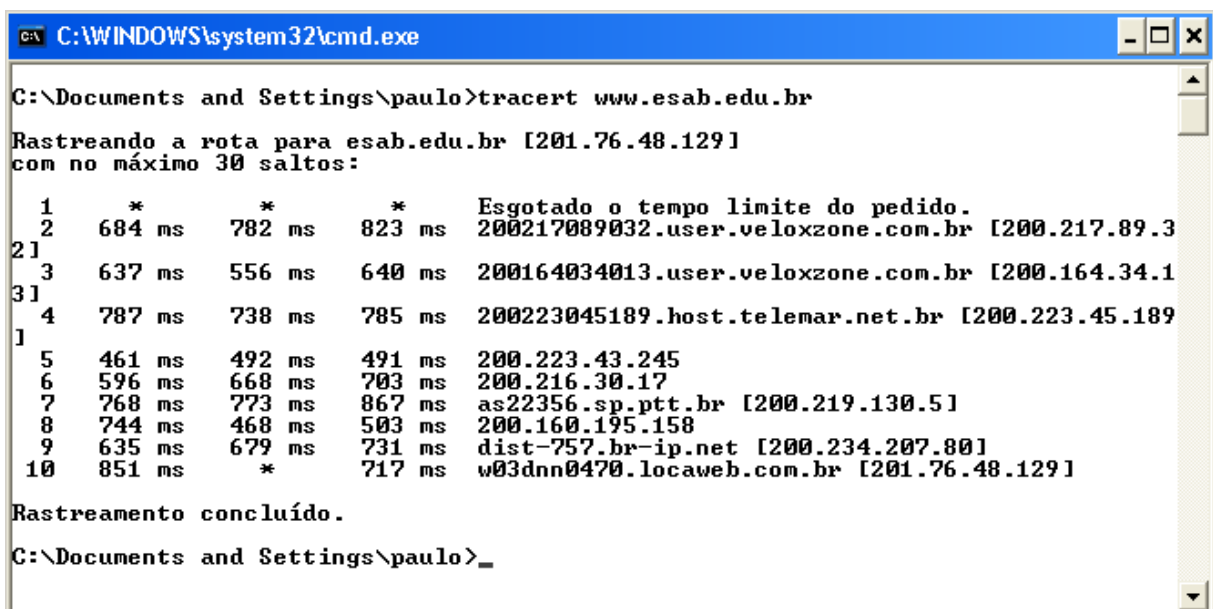
Esses ataques fazem com que os recursos do sistema sejam explorados de forma agressiva, o que pode impossibilitar a utilização da rede por usuários legítimos. Uma

técnica usada é o envio de pacotes específicos que podem causar a interrupção de determinado serviço (BURGESS, 2006).

4.10 – FIREWALKING

Segundo OLIVEIRA (2008), é uma técnica usada para obter informações de uma rede protegida por um *firewall*. Ela permite que pacotes pelas portas de um *gateway*, assim como verificar se pacotes com determinadas informações de controle pode passar pelo *firewall*. É possível ainda determinar os roteadores existentes antes do *firewall*, por causa da possibilidade de modificar o campo *TTL (Time To Live)* dos pacotes e as portas usadas, que permitem que as portas abertas pelo *firewall* sejam utilizadas para o mapeamento da rede.

O *firewalking* é um método implementado em uma ferramenta semelhante ao conhecido “*traceroute*” ou o “*tracert*” (no Windows).



```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\paulo>tracert www.esab.edu.br

Rastreando a rota para esab.edu.br [201.76.48.129]
com no máximo 30 saltos:

  1      *          *          *          Esgotado o tempo limite do pedido.
  2    684 ms    782 ms    823 ms    200217089032.user.veloxzone.com.br [200.217.89.3
2]
  3    637 ms    556 ms    640 ms    200164034013.user.veloxzone.com.br [200.164.34.1
3]
  4    787 ms    738 ms    785 ms    200223045189.host.telemar.net.br [200.223.45.189
]
  5    461 ms    492 ms    491 ms    200.223.43.245
  6    596 ms    668 ms    703 ms    200.216.30.17
  7    768 ms    773 ms    867 ms    as22356.sp.ptt.br [200.219.130.5]
  8    744 ms    468 ms    503 ms    200.160.195.158
  9    635 ms    679 ms    731 ms    dist-757.br-ip.net [200.234.207.80]
 10    851 ms          *          717 ms    w03dnn0470.locaweb.com.br [201.76.48.129]

Rastreamento concluído.

C:\Documents and Settings\paulo>_

```

Figura 5 – Ferramenta “*tracert*” no Windows
Fonte: Elaboração própria (2010)

Com algumas opções do próprio “*traceroute*”, há a possibilidade de adquirir informações sobre a rede. Caso um *firewall* permita apenas o tráfego de pacotes *ICMP* (normalmente o “*traceroute*” usa o *UDP*), basta utilizar a opção `-I` para que os

dados passem pelo *firewall*. O *traceroute* também permite que o rastreamento seja feito através de uma porta específica, o que pode ser usado em redes nas quais o *firewall* só permite o tráfego de pacotes *DNS*.

Dessa maneira, podem-se obter dados sobre as regras de filtragem dos *firewalls* e criar um mapeamento da topologia da rede. A utilização de servidores *proxy*, de *NAT* (*Network Address Translation*) e a proibição de pacotes *ICMP* são medidas que podem ser usadas para se defender do *firewalking* (NAKAMURA, 2003).

CAPÍTULO 5 – TÉCNICAS E FERRAMENTAS PARA DEFESA

5.1 – FIREWALL

A crescente necessidade das empresas em utilizar a *Internet* para realizar seus processos de negócio tem conduzido-as a interligarem suas *intranets* à rede mundial de computadores. Devido a isso, a preocupação com segurança e a importância de componentes de redes como *firewalls* tem aumentado.

Fazendo uma analogia com um antigo método de segurança medieval, TANENBAUM (2003, p. 583) conceitua o *firewall* da seguinte forma:

Os firewalls são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. Nas redes, é possível usar o mesmo artifício: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou de entrada da empresa é feito através de uma ponte levadiça eletrônica (*firewall*) [...]

O *firewall* é um equipamento que conecta duas ou mais redes, pelo qual circula todo o tráfego entre elas e por meio do qual é possível controlar, autenticar e registrar esse tráfego através de *logs*, permitindo auditorias nas redes. Dessa forma, o *firewall* pode ser utilizado para proteger a rede interna da organização de usuários externos, como também, controlar determinadas ações dos usuários internos na *Internet*.

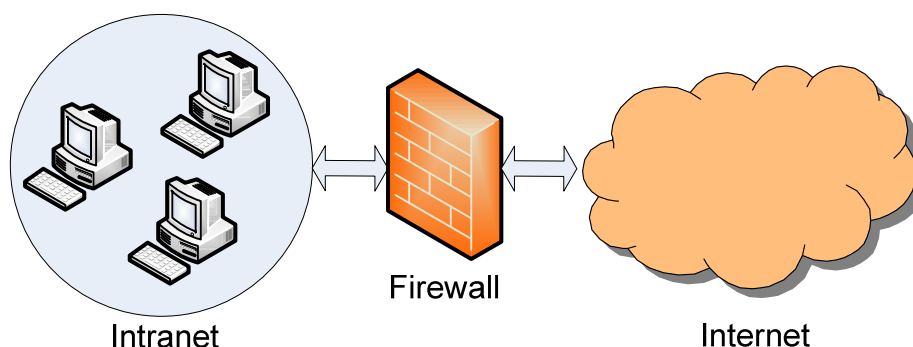


Figura 6 – Uso do *firewall* para proteger uma *intranet*
Fonte: Elaboração própria (2010)

5.2 – CRIPTOGRAFIA

A criptografia tem adquirido cada vez mais importância para a segurança das informações das empresas. A cifragem é o mecanismo para ocultar a mensagem original, que é escondida em uma mensagem com texto cifrado. A decifragem é o processo inverso de converter o texto cifrado de volta para o texto original. A criptografia permite que propriedades importantes para a proteção das informações das organizações sejam atingidas como: sigilo, autenticidade, não repúdio e integridade.

Os processos de cifragem e decifragem são efetuados por meio de algoritmos com funções matemáticas que transformam o texto claro, que pode ser lido, em texto cifrado, que é inteligível. Existem dois tipos de algoritmos, os de chave privada ou simétrica e os de chave pública ou assimétrica. Os algoritmos de chave privada são rápidos na execução, mas não permitem a certificação e assinatura digitais. E há também outros problemas como a dificuldade no envio das chaves secretas para os usuários por um canal de comunicação seguro e o uso de chaves secretas diferentes para cada tipo de comunicação ou mensagem, tornando seu gerenciamento bastante complexo (SILVA, 2003).

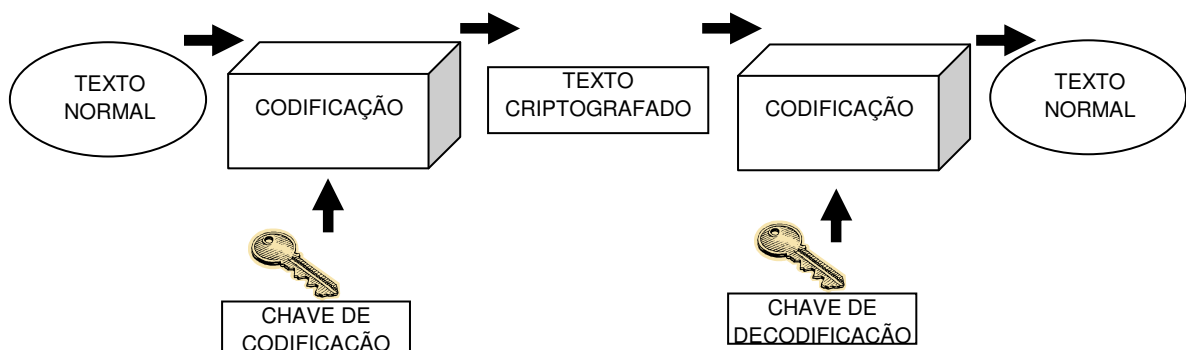


Figura 7 – Criptografia utilizando chaves
Fonte: Elaboração própria (2010)

Já os algoritmos de chave pública permitem que a assinatura e certificação digitais sejam utilizadas. As comunicações são efetuadas através do uso de dois pares de chaves diferentes, uma pública e outra privada para cada entidade. Uma mensagem

pode, por exemplo, ser cifrada usando uma chave pública e decifrada usando apenas a chave privada correspondente ou vice-versa. O algoritmo de chave assimétrica diminui o problema de troca de chaves, no entanto ele é mais lento que os algoritmos simétricos (OLIVEIRA, 2003).

5.3 – AUTENTICAÇÃO

No ambiente corporativo, a autenticação assume um papel muito importante ao validar a identificação dos funcionários. O acesso aos sistemas e recursos das empresas depende essencialmente desse processo de validação. Os fatores responsáveis por essa verificação são a identificação e autenticação que, junto com o *firewall*, formam a primeira linha de defesa em muitos sistemas.

A autenticação ou a validação da identidade do usuário, que fornece a autorização, pode ser feita usando três métodos (NAKAMURA, 2003):

- Baseando-se no que o usuário sabe: senhas ou chaves criptográficas;
- Baseando-se no que o usuário possui: cartão, *token*;
- Baseando-se nas características dos usuários (*biometria*): impressão digital, reconhecimento da retina, reconhecimento de voz, etc.

Todas essas formas de validar um usuário possuem pontos positivos e negativos, de modo que é recomendável uma autenticação com base em dois deles, quando o acesso requer maior grau de segurança (NAKAMURA, 2003).

5.4 – REDES PRIVADAS VIRTUAIS (VPNs)

A infra-estrutura de comunicação entre matriz, filiais, distribuidores, fornecedores clientes, parceiros de negócios e usuários móveis é muito importante dentro das empresas. É através dessa estrutura que são realizados os negócios da organização. Nessa malha de comunicações, pode-se observar que a cada novo integrante com o qual a organização precisa se relacionar, há o aumento do número de conexões e

dos custos envolvidos com as novas conexões dedicadas. Com isso, cresce a complexidade do sistema e há maior dificuldade no gerenciamento (SILVA, 2003).

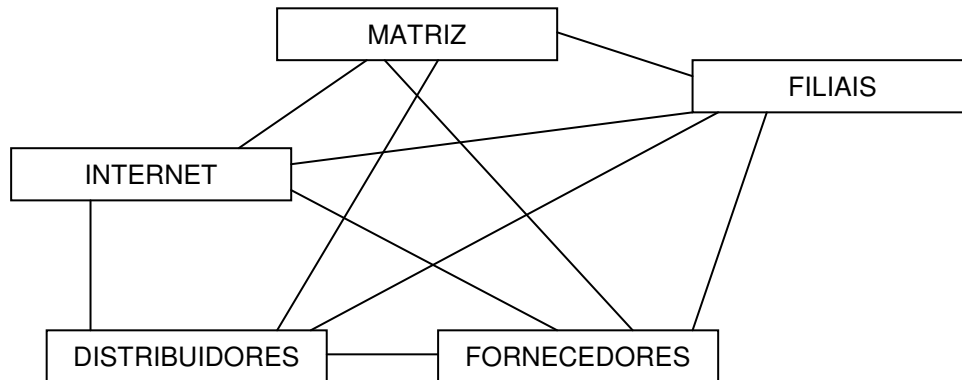


Figura 8 – A complexidade da rede de comunicações entre a matriz, filiais e parceiros de uma empresa

Fonte: Elaboração própria (2010)

Devido a esses problemas, ao mesmo tempo em que ocorre o aumento das conexões entre as corporações, podemos observar, também, um crescimento na utilização de redes públicas como a *Internet*, por exemplo. As redes públicas possuem custos relativamente mais baixos quando comparadas com as conexões dedicadas e formam o meio físico usado pelas redes privadas virtuais (*Virtual Private Networks – VPNs*).

Segundo TANENBAUM (2003, p. 583), o conceito de VPNs é:

São redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real.

As *VPNs* tornaram-se um fator importante dentro das empresas, pois utilizam uma rede pública para a comunicação no lugar das conexões privadas e estruturas de acesso remoto, que possuem custos mais altos. Através das redes privadas virtuais é possível criar conexões privadas, de forma que as comunicações passam a ser feitas por meio de uma única ligação com a rede pública.

Com utilização das *VPNs*, há mais simplicidade nas conexões porque somente uma conexão pública precisa ser gerenciada, ao contrário das diversas conexões apresentadas na figura 9.

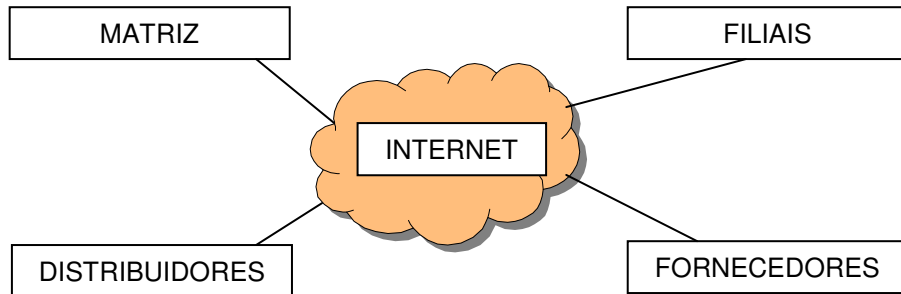


Figura 9 – Simplicidade nas ligações com a utilização de *VPNs*
 Fonte: Elaboração própria (2010)

Os dois principais aspectos que caracterizam a *VPN* são o tunelamento e a criptografia. O tunelamento é o que possibilita o uso de uma rede pública para o tráfego das informações, por meio da criação de um túnel virtual formado entre os dois entes da comunicação. A criptografia é usada para garantir o sigilo, autenticidade e integridade dos dados, sendo a base da segurança nos túneis *VPN*.

5.5 – SISTEMAS DE DETECÇÃO DE INTRUSÃO (*IDS*)

Um sistema de detecção de intrusão tem a função de identificar atividades suspeitas, anormais ou impróprias na rede. Ele funciona como uma câmera ou alarme contra invasões, efetuando a detecção através de algum conhecimento como desvios de comportamento ou assinaturas de ataques. Se os primeiros sinais de um ataque forem reconhecidos rapidamente, seus danos poderão ser minimizados. O *IDS* é capaz de oferecer meios para que a empresa melhore a proteção contra qualquer tipo de ataque, inclusive internos.

Existem três tipos de *IDS*, os baseados em host (*HIDS*), os baseados em rede (*NIDS*) e o *IDS* híbrido. O sistema de detecção de intrusão baseado em *host* monitora o sistema baseando-se em informações de arquivos de *logs* ou agentes de

auditoria. O *IDS* baseado em rede realiza o monitoramento verificando o tráfego do segmento de rede, normalmente com a interface de rede trabalhando em modo promíscuo, analisando o conteúdo dos pacotes e comparando com assinaturas ou padrões conhecidos. O *IDS* híbrido combina os pontos fortes do *HIDS* e do *NIDS* para oferecer melhor capacidade de detectar invasões (OLIVEIRA, 2008).

5.6 – DEFENDENDO-SE DE *SNIFFERS*

Alguns métodos podem ser usados para checar se um *sniffer* está sendo executado em um segmento de rede. Uma técnica interessante é o administrador do sistema acessar todos equipamentos desse segmento e verificar a existência de um determinado processo em execução. Entretanto, um atacante que estiver fazendo uso de um *sniffer* pode esconder esse processo, tornando-se difícil detectá-lo. A mesma coisa vale para a investigação de interfaces de redes que estão trabalhando em modo promíscuo.

A geração de tráfego de rede de senhas predeterminadas é outro método a ser usado, pois o atacante pode ser identificado através da utilização dessa senha. Mas é possível que ele faça enormes estragos antes de utilizar uma dessas senhas, o que torna essa técnica não muito eficiente, pelo fato da possibilidade dele possuir outras senhas de usuários legítimos.

Existem outros métodos que podem ser utilizados, sem a necessidade de acesso a cada máquina no segmento, para identificar remotamente a utilização dos *sniffers* (NAKAMURA, 2003):

- *MAC detection*: alguns sistemas operacionais possuem um erro de implementação no protocolo *TCP/IP*, no qual é utilizado apenas o endereço IP para entregar as mensagens, sem haver a conferência do endereço MAC, quando a interface está em modo promíscuo. Esse procedimento utiliza pacotes "*ICMP echo request*" com o endereço *IP* de uma máquina, mas com *MAC* falso. Se existir um *sniffer* sendo executado, ele estará em modo promíscuo, não vai conferir o endereço *MAC*, respondendo o "*ping*" e

podendo ser identificado. Se a correção a essa falha já foi aplicada ao sistema operacional, esse método não vai funcionar.

- *DNS detection*: aproveita a característica que alguns *sniffers* possuem de realizar *DNS* reverso. Assim, pacotes com endereços falsos são inseridos na rede e, se o *sniffer* captura-os, um pedido de *DNS* reverso é transmitido ao servidor *DNS*, que pode identificar a execução desse programas na rede. Esse procedimento pode detectar quantos *sniffers* estão em funcionamento entre diferentes segmentos de rede, mas não em que equipamentos eles estão.
- *Load detection*: Esse método explora o fato de que máquinas que estão executando *sniffers* demoram mais tempo para responder a requisições por estarem com um maior nível de processamento. Ele realiza uma análise estatística dos tempos de resposta a mensagens, comparando os tempos de respostas com pequeno tráfego na rede com o tráfego a ser capturado pelos *sniffers*. Os tempos são confrontados e se a diferença for muito grande, a máquina está com elevado grau de processamento, fato que pode estar sendo causado pela utilização de *sniffers*. Mas o tipo de pacote a ser usado nos testes deve ser selecionado com cuidado. Não há como usar, por exemplo, o *ICMP echo request*, por que a resposta é enviada pelo equipamento a partir da própria pilha *TCP/IP*, antes mesmo de chegar ao nível do usuário e dessa forma, não é possível medir o grau de processamento do nó de rede. É possível utilizar técnicas que funcionem no nível do usuário como comandos *FTP*. Mas em redes com bastante tráfego, esse método não funciona eficientemente, pois se torna mais difícil a comparação entre os tempos de resposta que ficam muito semelhantes.

O uso de *switches* ao invés de hubs também pode ser um bom procedimento para diminuir as chances de problemas relacionados às técnicas de *sniffing*. Como os *switchs* trabalham na camada 2 do modelo OSI, eles podem encaminhar os pacotes para portas determinadas. Já nos *hubs*, que trabalham na camada 1 do modelo OSI, isso não é possível.

No entanto, existem diversos métodos que tentam burlar as restrições colocadas pelos *switchs*, entre eles podemos destacar:

- Reconfiguração do *switch* utilizando o protocolo *SNMP*;
- Acesso administrativo ao *switch* e utilização procedimentos como engenharia social, ataques de força bruta, adivinhação de senhas, etc;
- Transmissão de muitos quadros usando endereços *MAC* ainda não utilizados, fazendo com que a tabela *MAC* do equipamento fique cheia e ele passe a trabalhar no modo *hub*.
- Transmissão de quadros com endereços *ARP* falsos, fazendo com que informações endereçadas a outros usuários sejam enviadas para a máquina do atacante, que retém os quadros e os retransmite para o equipamento verdadeiro, que nem se dá conta do ocorrido.

Mas com algumas medidas administrativas esses ataques podem ser minimizados. Limitar o acesso do administrador do equipamento apenas pela porta serial é um procedimento para prevenir o controle remoto não autorizado. Bloquear os acessos externos ou desabilitar o protocolo *SNMP*, assim como a utilização de listas de controle de acesso com endereços *MAC* e o uso de tabelas *ARP* estáticas também são técnicas aconselhadas. Considerar, porém, que o uso delas pode gerar uma maior carga de trabalho administrativo para gerenciá-las (NAKAMURA, 2003).

A capacidade de criar *LANs* Virtuais, comumente chamadas de *VLANs* (*Virtual LANs*), é outra característica muito utilizada nos switches. *VLANs* são redes separadas logicamente no mesmo equipamento. As *LANs* Virtuais podem estendidas a outros *switches* utilizando-se de uma técnica chamada *trunking*, que permite a existência de *VLANs* em diversos switches. Porém, o *trunking* pode trazer perigos à empresa, devido ao fato de tráfegos falsificados com identificadores de *VLANs* específicos podem ser transmitidos à rede tendo como objetivo o ataque a sistemas de outras *LANs* virtuais. Pode-se injetar quadros em uma *VLAN* para serem direcionados a outra (NAKAMURA, 2003).



Figura 10 – *Switch*
Fonte: Elaboração própria (2010)

Diante disso, As *LANs* virtuais não devem ser consideradas mecanismos de segurança, mas somente um meio de segmentar as redes para reduzir problemas de colisões e melhorar o uso de broadcast e *multicasts*. Em uma política de segurança fundamentada em camadas, é interessante o uso delas, no entanto a separação física das redes é muito mais eficaz.

5.7 – DEFENDENDO-SE DE ATAQUES FÍSICOS

Controlar o acesso físico das pessoas a locais estratégicos da organização é uma forma de diminuir a ocorrência deles. E esse controle deve ser planejado em diversos níveis. Por exemplo, o ingresso no prédio da empresa deve ser verificado para que a entrada da grande maioria das pessoas seja controlada. O controle de acesso a locais restritos e a movimentação dentro da instituição também deve ser controlada. Assim, é possível evitar o acesso a sistemas desbloqueados, estações de trabalho ou servidores. O acesso à estação de trabalho de um funcionário distraído pode ter conseqüências desastrosas, como no caso de um e-mail falso ser enviado a clientes ou parceiros de negócios. Também podem ser inseridos documentos falsos no sistema da empresa, assim como a cópia de projetos.

É preciso utilizar um sistema de identificação eficiente para que o controle de acesso aos servidores seja o mais limitado possível. Combinar a utilização de crachás com sistemas de biometria pode ser uma solução interessante, por que um crachá perdido não vai poder ser usado para acessos não permitidos à sala dos servidores.

É possível diminuir muito a quantidade de problemas relativos aos ataques físicos com esse tipo de procedimento, podendo ser melhorado ainda mais com o uso de câmeras de vídeo (NAKAMURA, 2003).



Figura 11 – Câmera de vídeo: pode ser usada para aumentar a segurança
Fonte: Elaboração própria (2010)

A permissão de acesso aos sistemas telefônicos também deve merecer atenção, pelo fato deles poderem permitir o ataque a sistemas importantes da corporação. Mais uma vez, a política de segurança desempenha um papel essencial para prevenir a ocorrência dos ataques físicos. Uma boa técnica é fazer com que os funcionários bloqueiem seus computadores quando não estão utilizando-os. Também é um bom hábito não deixar documentos confidenciais em cima das mesas, pois indivíduos de outras empresas podem se movimentar pelo ambiente interno adquirindo informações somente olhando para eles, fotografando ou roubando.

Outro procedimento utilizado em ataques físicos é o uso de analisadores de protocolos, os chamados *sniffers*, para captura de informações e senhas ou a instalação de um mecanismo para reter tudo o que o usuário digita. A perda de confidencialidade conseguida com uso desses processos é bastante encontrada nas instituições.

Além disso, a política de segurança deve prever situações relacionadas à disponibilidade de informações como incêndios, furacões, terremotos e enchentes

que podem causar a paralisação de atividades e perda de dinheiro (NAKAMURA, 2003).

5.8 – POLÍTICA DE SEGURANÇA

A política de segurança é um fator fundamental em todos os aspectos relacionados à proteção dos dados de uma organização. Sua elaboração é a primeira providência no processo de implementação da segurança das informações da empresa. É através dela que todos os fatores relacionados à proteção dos dados são determinados, por isso seu planejamento e elaboração demandam bastante trabalho. Porém, as maiores dificuldades não estão no planejamento ou elaboração dela, mas na sua implementação.

O planejamento da política de segurança deve ser abrangente e levar em consideração todas as normas e procedimentos da organização. Essas normas precisam determinar o que é permitido no sistema e os direitos dos funcionários além de controles e procedimentos necessários à proteção de dados. A figura abaixo mostra como se posiciona a política de segurança, acima das normas e procedimentos (NAKAMURA, 2003).

A política norteia de maneira global as ações e implementações futuras, ao passo que as normas abordam detalhes como conceitos, sistemas de controle e passos da implementação. Os procedimentos são empregados para que os funcionários possam realizar o que foi determinado na política e fazer com que os sistemas sejam configurados de acordo com as necessidades da empresa (NAKAMURA, 2003).

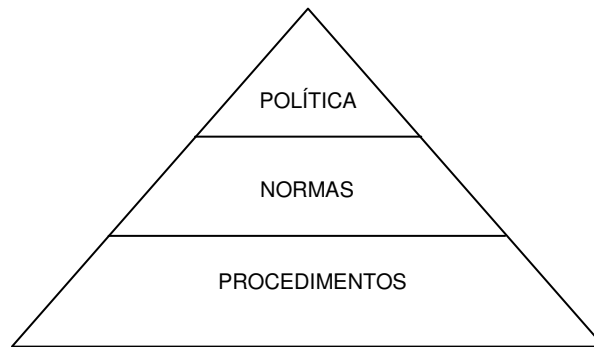


Figura 12 – Planejamento da política de segurança
Fonte: Elaboração própria (2010)

Alguns pontos são muito importantes na elaboração da política de segurança, entre eles podemos destacar (MITNICK, 2003):

- Conhecer prováveis inimigos, descobrindo suas intenções e como podem prejudicar a empresa;
- Contabilizar valores, determinando o quanto pode aumentar a quantidade de trabalho educacional e administrativo e a necessidade de aquisição novos recursos tecnológicos;
- Proteger os segredos da organização;
- Identificar os serviços estritamente necessários para o funcionamento da corporação;
- Considerar os aspectos humanos, realizando treinamento de segurança com todos os usuários antes de permitir seu acesso aos sistemas;
- Identificar seus pontos fracos;
- Não se esquecer da segurança física;

CAPÍTULO 6 – PROBLEMAS DE SEGURANÇA EM REDES SEM FIO

As redes sem fio, especificamente as redes *wi-fi* tornam-se a cada dia mais populares e é inegável a praticidade e mobilidade que elas proporcionam nos ambientes corporativos. Mas, juntamente com essa comodidade, vêm preocupações de segurança com a adoção dessa nova tecnologia. A implementação de uma rede sem fio pode trazer várias vantagens e às vezes é até inevitável. Porém, é importante que se compreenda as implicações de segurança de cada decisão tomada. Elas envolvem não somente questões de configurações, mas também de planejamento, projeto e escolha dos equipamentos que possuam as características desejáveis.

Sobre a vulnerabilidade das redes sem fio, TANENBAUM (2003, p. 583) apresenta uma situação:

[...] qualquer pessoa que queira espionar uma empresa pode dirigir até o estacionamento dos funcionários pela manhã, deixar um notebook capaz de reconhecer sinais 802.11 dentro do carro para registrar tudo que ouvir e partir no final do dia. À tarde, o disco rígido estará repleto de valiosas informações.

A tecnologia *wi-fi* ainda não amadureceu totalmente e, dessa forma, vários de seus padrões e protocolos ainda estão evoluindo e têm falhas. Assim como nas redes cabeadas, as ameaças às redes sem fios precisam ser conhecidas para que seus danos sejam minimizados através das soluções disponíveis e aplicação de boas práticas. A seguir, mostraremos alguns problemas de segurança envolvendo as redes *wi-fi*.

6.1 – VULNERABILIDADES DOS PROTOCOLOS WEP E WPA

De acordo com FERREIRA (2008), o protocolo *WEP* possui problemas de segurança graves. Os maiores problemas têm relação com o aspecto de ele usar uma chave única e estática sendo compartilhada entre todos os equipamentos da rede. Assim, se for preciso a substituição dessa chave, a troca pode ser bastante trabalhosa e muitas vezes tornar-se inviável. Além disso, o *WEP* utiliza chaves de criptografia

limitadas a 40 bits e foram apresentados problemas técnicos que permitem ataques ao próprio algoritmo. Sobre as vulnerabilidades do protocolo *WEP*, ROSS (2003, p. 193) afirma:

Como qualquer policial informaria a você, os cadeados são ótimos para manter as pessoas honestas afastadas, mas os ladrões perigosos sabem como arrombá-los. Um catálogo inteiro de ferramentas para violação de criptografia *WEP* pode ser encontrado facilmente na internet.

Já o protocolo *WPA* tem propriedades de segurança melhores que o *WEP*, mas mesmo assim ainda possui vulnerabilidades conhecidas. Entre elas pode-se destacar que o uso de senhas pequenas ou fáceis de adivinhar pode facilitar ataques de força bruta ou dicionário. Senhas com menos de 20 caracteres deixam a rede mais susceptível a este tipo de ataque. Apesar das melhorias implementadas no *WPA*, ainda há diversos pontos vulneráveis como problemas no armazenamento das chaves nos clientes, servidores ou concentradores (RUFINO, 2005).

6.2 – CONFIGURAÇÕES DE FÁBRICA

Os equipamentos de redes sem fio têm diversos mecanismos de segurança, porém muitos desses mecanismos não vêm ativados por padrão. Aparelhos configurados com as características padrões de fábrica podem permitir mais facilmente ataques, pois muitos itens de segurança podem estar desativados.

Uma grande preocupação dos fabricantes é tornar seus produtos amigáveis, como mostra TANENBAUM (2003, p. 585):

Grande parte do problema de segurança pode ter sua origem nos fabricantes de estações base sem fios (pontos de acesso) que tentam tornar seus produtos amigáveis para o usuário. Em geral, se o usuário retirar o dispositivo da caixa e o conectar à tomada da rede elétrica, ele começará a operar de imediato — quase sempre sem qualquer segurança, revelando segredos para todo mundo que estiver dentro do alcance de rádio. Se ele for conectado a uma rede Ethernet, todo tráfego da Ethernet também aparecerá de repente no estacionamento. A rede sem fio é um sonho que se tornou realidade para o espião: dados gratuitos sem qualquer trabalho. Por essa razão, não é preciso dizer que a segurança é ainda mais importante para sistemas sem fios que para sistemas fisicamente conectados.

Apesar disso, muitos administradores implantam esses aparelhos nas corporações sem realizar nenhuma alteração nas suas configurações. Eles, normalmente, vêm configurados com endereço *IP* e senhas de administração padronizadas e, se esses itens não forem alterados, um atacante pode utilizar-se deles para verificar características do aparelho ou modificar suas configurações. Em redes que usam o padrão segurança *WEP*, por exemplo, se o administrador não alterar o valores das chaves *WEP* pré-configurados de fábrica nos equipamentos, poderá deixar a rede bastante vulnerável a ataques. Um atacante pode facilmente ter acesso a essas informações que podem ser encontradas em documentos públicos e manuais. Medidas importantes devem ser realizadas como alteração das chaves *WEP* ou *WPA*, contas administrativas e do *SSID* para não permitir a identificação de características úteis a ataques. Outro serviço que geralmente vem ativado por padrão em muitos aparelhos é o *SNMP*. Ele pode revelar grande quantidade de informações sobre o equipamento e, até mesmo, permitir a modificação de determinadas configurações remotamente. Informações como quantidade de clientes ou dispositivos conectados e seus endereços *MAC* e *IP* podem ser obtidos por um atacante, caso o protocolo *SNMP* esteja habilitado.

Apesar das diversas semelhanças entre as redes *wi-fi* e cabeadas, existem muitas características que são novas e até mesmo administradores com muita experiência vêm enfrentando dificuldades para configurar o ambiente de forma segura. Além disso, o fato de muitos equipamentos virem com todas as possibilidades de conexão ativadas e sem nenhum mecanismo de segurança habilitado, às vezes, torna mais complicado a tarefa de construir uma rede segura e funcional (RUFINO, 2005).

6.3 – ACESSO NÃO PERMITIDO EM CONFIGURAÇÕES BÁSICAS

Em situações o concentrador foi configurado para aceitar qualquer tipo de conexão, basta que o atacante disponha de um equipamento com interface sem fio utilizando o mesmo padrão do ambiente para ele ter acesso não autorizado à rede.

E até mesmo quando o *SSID (Service Set Identifier)* não é transmitido pelo concentrador, o atacante poderá realizar escuta do tráfego para conseguir essa informação e conectar-se ao equipamento. Existem algumas ferramentas específicas para redes sem fio que mostram as redes existentes em uma determinada área e suas características.

Utilizar configurações básicas em equipamentos *wi-fi* efetivamente não oferece segurança alguma. Para ter uma rede sem fio com um nível de segurança aceitável é preciso prestar bastante atenção nas configurações de cada aparelho, alterando-as quando preciso, e usar recursos adicionais como criptografia e autenticação forte que não fazem parte da configuração básica (RUFINO, 2005).

Para proteger-se de ataques, é preciso configurar os mecanismos de segurança dos equipamentos *wi-fi*, como aponta SANCHES (2005, p. 234):

Na maioria dos equipamentos os recursos de segurança vêm desativados a fim de que a rede funcione imediatamente após sua instalação, assim antes de iniciar a utilização propriamente de uma rede sem fios, devemos configurar todas as opções de segurança.

6.4 – ENVIO E RECEPÇÃO DE SINAL

Nas redes *wi-fi*, a posição dos equipamentos é um fator muito importante em relação à segurança e qualidade da rede. É fácil perceber como esse é um aspecto relevante, visto que, como se sabe, o sinal é transmitido em várias direções. Assim, um ponto de acesso *wi-fi* posicionado dentro de uma sala transmitirá o sinal tanto para dentro quanto para fora dela, mesmo que o administrador não deseje isso. Uma boa maneira de minimizar essa característica indesejável é posicionar o aparelho o mais próximo possível do centro do local, o que pode também melhorar o aproveitamento do sinal pelas estações da sala (RUFINO, 2005).



Figura 13 – Um atacante pode realizar um ataque mesmo no ambiente externo à empresa
 Fonte: Elaboração própria (2010)

Um ponto de acesso mal localizado pode oferecer um sinal de ótima qualidade a um atacante externo ao ambiente. Vale salientar, no entanto, que se o invasor fizer uso de equipamentos com melhor recepção, por exemplo, o sinal fraco fora da sala poderá não impedir seu acesso à rede.

6.5 – MAPEAMENTO DO AMBIENTE

Para adquirir maiores informações sobre a rede a ser atacada, uma das primeiras providências do atacante é realizar um mapeamento do ambiente. Esse mapeamento vai oferecer a ele características importantes do ambiente computacional e, dessa forma, permitir ataques mais precisos e com menores riscos de serem identificados. O sucesso dessa técnica vai depender dos mecanismos de segurança utilizados na rede *wi-fi* (RUFINO, 2005).

6.6 – CAPTURA DE TRÁFEGO

Como os dados transmitidos nas redes sem fio viajam pelo ar, eles são muito mais fáceis de ser capturados. É importante que as informações sejam cifradas para que o conteúdo do tráfego não seja conhecido por pessoas não autorizadas. Um atacante localizado na área de cobertura da rede e de posse de um computador ou

notebook e um *software* para captura de tráfego pode ter acesso a esses dados. Os mesmos programas utilizados para captura de pacotes usados nas redes cabeadas também podem ser usados nas redes *wi-fi*, porque quase todos funcionam com qualquer interface de rede (RUFINO, 2005).

6.7 – NEGAÇÃO DE SERVIÇO

Muitas vezes, há grande preocupação com a proteção contra acessos não permitidos e privacidade dos usuários e esquece-se dos ataques de negação de serviço. Nesse método de ataque, não é preciso invadir a rede, mas ele pode trazer graves transtornos ao ambiente.

Muitos administradores acreditam que as redes sem fio estariam livres desse tipo de ataque, pois apenas com equipamentos especiais e caros o atacante conseguiria efetuarlo. No entanto, o que se observa na prática é que até mesmo dispositivos usando a tecnologia *bluetooth* podem gerar retardo e, em determinadas situações, impedir o acesso a alguns aparelhos da rede sem fio. Foi observado, em testes de laboratório, que equipamentos *bluetooth* de classe 1, que tem alcance aproximado de 100 metros, quando colocados próximo a concentradores *wi-fi*, causam bastante interferência. Apesar de haverem diversos métodos de diminuir as interferências, eles não são suficientes quando toda ou uma grande faixa da frequência utilizada é preenchida com ruído. Se o aparelho do atacante tem potência suficiente para transmitir um sinal que preencha grande parte ou toda a faixa de frequência utilizada pelos aparelhos da rede, mesmo que o protocolo detecte ruído em um canal, não vai restar nenhum outro intervalo livre para transmitir, porque todo espaço foi preenchido pelo sinal do indivíduo que tenta o ataque (RUFINO, 2005).

6.8 – APARELHOS *WI-FI* EM REDES CABEADAS

Cresce cada vez mais, a quantidade de equipamentos que já são fabricados com algum tipo de interface de rede sem fio incorporada. Diante disso, também

aumentam as situações onde esses aparelhos podem servir de ponte para um ataque às redes cabeadas. Através de um *notebook*, por exemplo, um atacante pode conectar-se a rede cabeada de uma organização e permitir que um segundo atacante tenha acesso a ela, necessitando apenas da ativação da placa *wi-fi* para funcionar no modo *ad-hoc* e permitir o roteamento para a rede cabeada.

Até mesmo o próprio funcionário da empresa pode facilitar o acesso de usuários externos, apenas mantendo a placa de rede sem fio ligada buscando um concentrador ou outro computador em modo *ad-hoc*.

Outra situação onde um ataque poderia ocorrer seria quando o funcionário utiliza a rede sem fio de um local público e, ao voltar para ao trabalho, seu computador tenta conectar-se ao concentrado utilizado anteriormente. O atacante pode descobrir esse sinal e configurar um falso concentrador com as propriedades pedidas pela interface cliente para fazer com que o computador do funcionário conecte-se ao dispositivo falso. Assim, se o usuário também estiver conectado à rede cabeada, o atacante poderá acessá-la usando o computador do funcionário como *gateway* (RUFINO, 2005).

6.9 – SEGURANÇA FÍSICA

Muitos administradores de rede dão muita atenção à segurança lógica e esquecem-se da segurança física, principalmente devido à segurança física estar relacionada a outros departamentos da empresa. Se nas redes cabeadas, a segurança física é um componente bastante importante, nas redes sem fio ela se torna ainda mais valiosa, pois a área de cobertura física cresce consideravelmente. Com a implementação de uma rede sem fio, o que antes podia ser controlado através do controle de acesso à portaria, recepção ou acesso físico a um computador da empresa, agora precisa ser controlado numa área de dezenas ou centenas de metros ao redor da corporação, dependendo da área de abrangência da rede. Fatores que anteriormente podiam ser relevados, como a posição de alguns equipamentos, que agora precisam ser verificados para dificultar ataques e acessos não autorizados.

É preciso prestar bastante atenção em aspectos como o padrão utilizado e a potência do sinal configurada. A grande maioria dos equipamentos de rede sem fio permite a escolha de valores intermediários entre a potência mínima e máxima suportada. Outro que deve ser levado em consideração é a utilização de interfaces ou antenas mais potentes que podem aumentar a distância da recepção. Dessa maneira, somente checar até onde o sinal alcança não é suficiente para assegurar que ele não será captado a uma distância maior, pois um atacante possuidor de uma antena melhor ou interface mais potente poderá conseguir acesso ao sinal.

Portanto, apenas testar até onde o sinal chega, não é o bastante para prevenir ataques, porque se o atacante usar um aparelho com propriedades diferentes ou mais moderno poderá receber o sinal em áreas não reveladas nos testes (RUFINO, 2005).

CAPÍTULO 7 – TÉCNICAS DE DEFESA EM REDES SEM FIO

O acesso ao concentrador da rede sem fio é um ponto que merece bastante atenção, pois um acesso não permitido a ele pode colocar em risco a segurança, impossibilitar a comunicação com os clientes, permitir o redirecionamento de tráfego para outra máquina, a retirada de mecanismos de segurança e autorizar o acesso à rede por máquinas originalmente não autorizadas, entre outros problemas.

No caso do concentrador, a defesa consiste na proteção contra ataques de negação de serviço ou acessos não autorizados, mas também devem ser considerados a privacidade dos clientes e outros tipos de ataque. O concentrador *wi-fi* geralmente funciona como um elo entre a rede sem fio e a cabeada, sendo acessado por ambas e este é mais um problema a ser solucionado, pois critérios de acesso e monitoramento são diferentes para cada um dos lados (RUFINO, 2005).

Entre as medidas que podemos tomar para evitar ou minimizar os problemas de segurança relacionados aos concentradores sem fio, temos:

- Alterar o nome *ESSID* padrão: O atacante em princípio desconhece algumas informações técnicas do concentrador, que geralmente vêm no nome padrão, dificultando a execução do ataque. A modificação do nome padrão é uma forma eficaz de, pelo menos, retardar uma invasão, podendo oferecer tempo para o administrador identificá-la e tomar as medidas necessárias. No entanto, ao alterar o nome *ESSID* padrão, o administrador deve considerar que informações no novo nome que permitam identificar características da empresa podem acarretar ainda mais problemas. Ao mudar o nome, deve-se escolher um que não revele nem a organização nem o equipamento (ROSS, 2003);
- Desativar a difusão do envio do *ESSID*: essa medida busca dificultar ataques tentando esconder o nome da rede, pois dessa forma o provável atacante tem de saber o nome da rede ao qual o concentrador faz parte para realizar um ataque. Essa forma de promover segurança pode ser eficiente em certas situações, principalmente quando combinada com outras técnicas, mas essa medida, sozinha, pode não ter efeito algum porque existem outras maneiras

de se conhecer o *SSID* da rede-alvo, como por escuta de tráfego, por exemplo (SANCHES, 2005);

- Desabilitar acessos ao concentrador via rede sem fio: como a maioria dos concentradores permite sua configuração por *HTTP* e alguns por *telnet* e não há uma forma alternativa (cifrada) para esse acesso, é recomendável desativar essas opções no lado da rede sem fio. Essa medida pode evitar que dados como nomes de usuários e senhas venham a ser capturados por um invasor. Vale lembrar, que a rede cabeada deve possuir outros mecanismos de proteção que possibilitem o monitoramento e autenticação de usuários para poder restringir e identificar acessos ao concentrador (RUFINO, 2005);
- Alteração do endereço *MAC*: alguns concentradores oferecem a possibilidade de alterar o endereço *MAC*, fazendo com que a relação dele, geralmente feita por ferramentas de varredura, com o fabricante do equipamento seja desfeita (SANCHES, 2005);
- Desabilitar comunicação entre os clientes: esse mecanismo impede o acesso de um cliente a outros conectados ao mesmo concentrador, bloqueando o ataque direto de um usuário a outro. Entretanto, não impede a captura de pacotes e não garante a privacidade dos usuários (RUFINO, 2005);
- Ignorar clientes que enviam *SSID* igual a “*ANY*”: *SSID* com *ANY* geralmente indica um cliente à procura de qualquer concentrador disponível e pode até um atacante explorando a rede em busca de informações. Alguns concentradores permitem desabilitar a conexão com clientes com *SSID* igual a “*ANY*”, sendo interessante pesquisar no manual do equipamento se essa funcionalidade está presente (RUFINO, 2005).

CAPÍTULO 8 – A IMPORTÂNCIA DO TREINAMENTO DOS FUNCIONÁRIOS DA ORGANIZAÇÃO

Uma organização pode estar utilizando as melhores tecnologias de segurança, mas mesmo assim ainda estar muito vulnerável a ataques ou perdas de informações, se não realizar o treinamento de seus empregados com procedimentos que minimizem evitem esses problemas. Esse treinamento, que deve ser orientado pela política de segurança da empresa, devendo ser estendido a todos na corporação, como afirma MITNICK (2003, p. 28):

O treinamento de segurança com relação à política da empresa criada para proteger o ativo de informações precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao ativo de IT da empresa.

Na concepção de SILVA (2003, p. 184), “O treinamento é indispensável quando se pensa em segurança”. Os funcionários precisam ser treinados a não ajudar pessoas que não conheçam pessoalmente, mesmo que elas afirmem ser um executivo. É preciso também, compreender o perigo de atender pedidos para realizar ações em computadores de outras pessoas. As corporações devem ter políticas e procedimentos que orientem seus funcionários quanto a operações envolvendo computadores ou equipamentos relacionados, pois a execução de um determinado pedido pode levar à propagação de informações confidenciais ou ocasionar problemas ao ambiente computacional. Todos precisam conhecer as ameaças e vulnerabilidades existentes no mundo da segurança computacional. Além disso, os guardas responsáveis pela segurança física da empresa também precisam ser treinados em segurança da informação, já que muitas vezes têm acesso físico a todos os equipamentos da organização. E ainda, sobre a implantação de sistemas de informações nas empresas, O'BRIEN (2004, p. 345) afirma que “O treinamento é uma atividade vital da implantação. O pessoal de SI, tais como consultores do usuário, deve se certificar de que os usuários finais sejam treinados [...] ou sua implantação fracassará”.

As tecnologias de segurança podem impedir certos tipos de ataques, mas os que se utilizam da engenharia social só são efetivamente minimizados quando há o

treinamento e conscientização dos empregados quanto à política de segurança. Nesse sentido MITNICK (2003, p. 113) diz:

Os códigos de segurança verbais são equivalentes às senhas, pois fornecem um meio conveniente e confiável de proteger os dados. Mas os empregados precisam conhecer os truques que os engenheiros sociais usam e devem ser treinados para não revelar os segredos de estado.

Alguns pontos são importantes nesse treinamento como (NAKAMURA, 2003):

- Instruir os empregados a verificar a identidade da pessoa que faz uma determinada solicitação e se está autorizada a fazê-la;
- Os procedimentos usados pelos atacantes que utilizam engenharia social para atingir seus alvos;
- Como identificar ataque de engenharia social;
- Como proceder no caso de uma solicitação suspeita;
- A quem se dirigir, caso identifique um ataque;
- A necessidade de questionar a todos os que fazem algum pedido suspeito, independente do cargo que ocupem;
- A importância de confirmar a identidade e autoridade de qualquer indivíduo que faça algum pedido de informações ou para realizar determinada ação;
- Métodos para proteger as informações confidenciais da empresa;
- Apresentação e explicação da política de segurança da organização;
- Informar sobre a obrigatoriedade dos funcionários em cumprir as normas, procedimentos e a política de segurança da empresa, assim como, as conseqüências quanto ao não cumprimento desses itens.
- Apresentação da política relacionada a senhas;
- O descarte adequado de mídias e documentos, principalmente os confidenciais, que não são mais úteis;
- A política relacionada ao uso do *e-mail*, apresentando formas de evitar ataque com vírus, *worms*, cavalos de tróia, etc.

CONCLUSÃO

Iniciamos esse trabalho com o intuito de identificar os problemas e soluções relacionados à segurança dos dados nas corporações. Na busca para solucionar essa questão, verificamos a grande necessidade das organizações de compartilhar e acessar informações de qualquer lugar do mundo atualmente. Além disso, cada vez mais as organizações estão diminuindo o uso do papel, digitalizando todas as suas informações e realizando suas transações e negócios através da *internet*, com a ligação de suas *intranets* à rede mundial de computadores.

Observamos que as empresas tradicionais, antes baseadas apenas no mundo do papel e de alguma forma isoladas do mundo exterior, hoje estão a caminho da transformação em empresas digitais, onde o papel é abolido e todas as transações são realizadas eletronicamente. Nesse processo, percebemos que aparecem vantagens, mas também surgem alguns problemas que precisam ser considerados. Os principais benefícios observados são rapidez nas transações e a facilidade de acesso aos dados de qualquer parte do planeta. Os problemas que surgem nesse processo de transformação e foram abordados nesse trabalho de pesquisa estão relacionados à maior preocupação com a segurança dos dados.

Compreendemos que, agora, como os dados não estão mais no papel e sim gravados digitalmente, as corporações precisam utilizar equipamentos para proteger seus dados de danos causados pela eletricidade, por pessoas que utilizam a internet para acessar ou destruir dados importantes e até de catástrofes como terremotos e enchentes.

Assim, a segurança dos dados adquire considerável relevância, pois alguém que queira acessar dados confidenciais ou atacar o sistema de uma organização pode fazer isso de qualquer lugar do mundo. Vimos a variedade de indivíduos e técnicas que podem causar danos aos negócios das empresas digitais. Ao identificar esses atacantes e procedimentos de ataque, concluímos o quanto é importante as organizações adotarem as soluções de defesa existentes no mercado que foram apresentadas nesse estudo.

E atualmente com o maior uso das redes sem fio, percebemos a grande necessidade de configurar corretamente as redes wireless para evitar os problemas de segurança destas demonstrados no estudo realizado.

Compreendemos, também, que o treinamento de todos os usuários dos sistemas computacionais das organizações é outro fator de grande relevância para a proteção das informações empresariais, pois de nada adianta ter os melhores equipamentos e procedimentos se os recursos humanos da empresa não estão preparados para lidar com os sistemas de informações, situações perigosas e pessoas mal-intencionadas.

Diante do que foi apresentado, evidencia-se a importância do estudo e da pesquisa em segurança das informações nas redes de computadores para que se identifiquem novas vulnerabilidades dos sistemas e sejam desenvolvidas outras formas de evitar ataques às empresas digitais. Por último, recomendamos a todos os que pesquisam ou trabalham nessa área, a necessidade da atualização constante de seus conhecimentos, pois todos os dias surgem notícias de novas vulnerabilidades nos sistemas computacionais. Portanto, é imprescindível a todos conhecer os novos pontos fracos ou formas de ataque que surgem dia a dia, para defender adequadamente os sistemas de informações.

REFERÊNCIAS

- BURGESS, M. **Princípios de Administração de Redes e Sistemas**. Rio de Janeiro: LTC, 2006.
- FERREIRA, F. C. **Projeto de Redes**. Vila Velha: ESAB, 2008. (Módulo de Projeto de Redes, Curso de Pós-graduação Lato-sensu em Redes de Computadores, Escola Superior Aberta do Brasil).
- ENERGYBRAZ. **Problemas que atingem a rede elétrica**. Disponível em: <<http://www.energybraz.com.br> >. Acesso em: 06 de setembro de 2010.
- HEUSER, C. A. **Projeto de Banco de Dados**. Porto Alegre: Sagra Luzzato, 2004.
- KORTH, H. F.; SILBERSCHATZ, A.; SUDARSHAN, S. **Sistema de Banco de Dados**. São Paulo: Campus, 2005.
- LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação Gerenciais - administrando a empresa digital**. São Paulo: Pearson Education, 2004.
- MITNICK, K. D.; SIMON, W. L. **Arte de Enganar, A**. Rio de Janeiro: Makron, 2003.
- NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Berkeley, 2003.
- O'BRIEN, J. A. **Sistemas de informação e as decisões gerenciais na era da Internet**. São Paulo: Saraiva, 2004.
- OLIVEIRA, G. **Segurança de Redes**. Vila Velha: ESAB, 2008. (Módulo de Segurança de Redes, Curso de Pós-graduação Lato-sensu em Redes de Computadores, Escola Superior Aberta do Brasil).
- ROSS, J. **O livro de Wi-Fi : instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003.
- RUFINO, N. M. O. **Segurança em redes sem fio : aprenda a proteger suas informações em ambientes wi-fi e bluetooth**. São Paulo: Novatec, 2005.
- SANCHES, C. A. **Projetando redes WLAN : conceitos e práticas**. São Paulo: Érica, 2005.
- SILVA, S. S. **VPN – Virtual Private Network – Aprenda a construir redes privadas virtuais em plataformas linux e windows**. São Paulo: Novatec, 2003.
- TANENBAUM, A. **Redes de computadores**. Rio de Janeiro: Campus, 2003.
- VALENTE, C. **Fundamentos de Sistemas de Informação**. Vila Velha: ESAB, 2007. (Módulo de Fundamentos de Sistemas de Informação, Curso de Pós-graduação Lato-sensu em Redes de Computadores, Escola Superior Aberta do Brasil).