ANTÔNIO LEMOS RÉGIS

IGNORÂNCIA, PRUDÊNCIA E SABEDORIA NA RESISTÊNCIA DA EMPRESA AO USO DA INTERNET

Florianópolis – SC

2001

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Antônio Lemos Régis

IGNORÂNCIA, PRUDÊNCIA E SABEDORIA NA RESISTÊNCIA DA EMPRESA AO USO DA INTERNET

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Professor Orientador
Luiz Fernando Jacintho Maia

Florianópolis, Fevereiro de 2001

IGNORÂNCIA, PRUDÊNCIA E SABEDORIA NA RESISTÊNCIA DA EMPRESA AO USO DA INTERNET

Antônio Lemos Régis

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof Dr. Fernando Álvaro Ostuni Gauthier (Coordenador)

Banca Examinadora

_____

Prof Dr. Luiz Fernando Jacintho Maia (orientador)

_____

Prof Dr. Rogério Cid Bastos

_____

Prof. Dr. João Bosco da Motta Alves

Dedicatória:

Dedico este trabalho a minha esposa Rozângela, aos meus filhos Wellington, Paulo Henrique, Elaine e aos meus pais que dedicaram tempos preciosos de suas vidas para a minha educação.

Agradecimentos

Este trabalho não teria sido viabilizado sem a ajuda de muitos que nos apoiaram no decorrer desta jornada, aos quais apresento meu reconhecimento:

Ao Nosso Grande Pai Celestial, pela proteção divina e pela iluminação nos momentos em que a inspiração se fazia distante;

Prof. Dr. Luis Fernando Jacinto Maia meu Orientador, por compartilhar seu valioso conhecimento e por ter acreditado no meu esforço;

Raimundo Josedi Ramos Veloso Gerentes de Informática do Sebrae, pelas informações do sistema de segurança instalados em sua instituição e pelo material fornecido para pesquisa;

Aos amigos e colegas de trabalho da Coopertec, pelo incentivo e encorajamento para que eu caminhasse até a conclusão desta jornada;

SUMÁRIO

Resumo

Com certeza o bem mais valioso de uma empresa são suas informações operacionais referentes a produtos, serviços, clientes etc. Por isso estas informações devem receber uma atenção especial quanto a sua segurança, contra acessos indevidos não autorizados que podem causar grandes prejuízos. Esse risco de danos à informação de uma empresa aumentou com o surgimento do comercio eletrônico, houve uma época em que a internet era um lugar pequeno e amigável, lembrando uma cidade do interior. As pessoas podiam deixar suas portas virtuais abertas, e os vizinhos só entravam para dizer olá. Com o passar do tempo, muitas outras pessoas se mudaram para essa cidade, até que um dia alguém notou que agora a internet se parece com a cidade de São Paulo. Nessa nova internet, as pessoas são forçadas a passar o ferrolho nas portas, instalar sistemas de alarme, comprar cães de guarda e dirigir seus carros com as portas trancadas.Com essa analogia podemos, agora, entender melhor tanto o propósito do trabalho aqui apresentado, como também o intuito de se desenvolver sistemas para garantir a segurança e a integridade dos dados contidos em um computador ou em uma rede de computadores, um desses sistemas de proteção mais difundidos atualmente é o firewall. O firewall é o elemento que delimita a defesa de perímetro, pois ele quando bem configurado indica quem irá acessar uma rede, até que ponto dessa rede um usuário pode ir, qual serviço pode ter acesso, contudo ainda é necessário ter outros meios de segurança como criptografia, autenticação, assinatura digital e encapsulamento da informação, para aumentar a segurança das informações contra ataque de intrusos. A vulnerabilidade das informações de uma instituição sempre vão existir por não se ter sistemas de segurança totalmente perfeitos e funcionários totalmente honestos, mas existem meios e formas de se criar um ambiente seguro para as informações da corporação, quando as regras de segurança são bem elaboradas e implantadas segundo os critérios previamente estudados e pré-estabelecidos, o êxito com a segurança da informação é total, a partir deste principio é que desenvolvemos este trabalho.

Abstract

The most valuable wealth of a company is their operational information regarding products, services, customers etc. This kind of information must receive special attention regarding its safety, against improper or non authorized accesses that can cause great damages. This risk of damages to the information of a company increased with the appearance of the electronic commerce. There was a time in that the Internet was a small and friendly place, reminding a country town. The people could let opened their virtual doors, and the neighbors entered only to say hello. In the course of time, many other people moved in that town. One day somebody realized that now the internet resembles the city of São Paulo. In that new internet, the people are forced lock the doors, to install alarm systems, to buy watchdogs and to drive their cars with the locked doors. We can use this analogy to understand the purpose of this work as well as the intention of developing systems to guarantee the safety and the integrity of the data contained in a computer or in a net of computers. Nowadays, the most spread protection system is the firewall. The firewall is the element that delimits the perimeter defense. It when correctly configured, indicates who will access a net, to what extent of that net the user can go, which service can it have access. However it is still necessary to have other resources to guarantee the data safety and loss prevention as cryptography, authentication, digital signature and encapsulation of the information. These resources increase the safety of the information against attacks of intruders. The vulnerability of the information of an institution will always exist, considering there will never exist totally perfect safety systems and totally honest employees, but there are means and forms of creating a safe atmosphere for the information of the corporation, when safety's rules are well elaborated and implanted according to a previously studied criteria, by that means, there will be total success with the information safety and loss prevention and this is the theoretical elaboration axis of this work.

INTRODUÇÃO

O presente trabalho tem por objetivo a apresentação dos conceitos básicos do contexto de ***Segurança em Informática***: o valor da informação, concepção de segurança os principais riscos, tais como acesso lógico, acesso físico etc. medidas preventivas e procedimentos corretivos do ambiente de redes **Intranets e Internet**.

Inicialmente, damos uma visão geral da necessidade de segurança e de **política de segurança** e **plano de contingência** na empresa. A seguir, é enfatizado o aspecto crítico de acesso lógico e físico aos sistemas, terminando com o emergente e polêmico tema **segurança na Internet**, explorando a vulnerabilidade da rede, o uso de criptografia, o problema da autenticação de usuários e a necessidade do uso de firewalls. As medidas de segurança mais amplamente empregadas e publicadas em uso são antivírus, backup e firewall. São ferramentas em questão para segurança de um sistema. Elas fornecem um certo nível de proteção e são, em geral, uma maneira de implementar a política de segurança no nível de rede. O nível de segurança que um firewall fornece pode variar tanto quanto o nível de segurança em uma máquina particular. Existe o tradicional "trade-off" entre segurança, facilidade de uso, custo elevados, complexidade, etc.

Um firewall geralmente é uma maneira de construir uma parede entre uma parte de uma rede, uma rede interna de uma empresa, por exemplo, e outra parte, a Internet global, por exemplo. A única característica sobre esta parede é que precisam existir maneiras para algum tráfego com características particulares passarem através de portas cuidadosamente monitoradas ("gateways"). A parte difícil é estabelecer o critério pelo qual os pacotes são permitidos ou negados acesso pelas portas. Livros escritos sobre firewall usam terminologias diferentes para descrever as várias formas de firewalls. Isto pode ser confuso para administradores de sistemas que não são familiares com firewalls. Uma discussão referente a capacidades de uma marca particular de roteador, executando uma versão de software específica está fora do escopo deste documento. Para melhor segurança, os filtros geralmente restringem acesso entre as duas redes conectadas a apenas um host, o bastion host. Só é possível ter acesso para a outra rede através deste bastion host. Como somente este host, em lugar de algumas centenas de hostes, pode ser

atacado, é mais fácil manter um certo nível de segurança, pois somente este host tem que ser muito cuidadosamente protegido. Para tornar disponíveis recursos para legitimar usuários através deste firewall, serviços têm que ser passados adiante pelo bastion host. Alguns servidores têm esta capacidade embutida (como servidores DNS ou servidores SMTP), para outros serviços (por exemplo, Telnet, FTP, etc.), servidores proxy podem ser usados para permitir acesso aos recursos através do firewall de modo seguro.

Firewalls são pensados como uma maneira de manter intrusos do lado de fora, mas eles são usados geralmente como uma maneira de legitimar usuários em um site. Existem muitos exemplos onde um usuário válido poderia precisar acessar regularmente o site "home" durante viagens para apresentações e conferências, etc. Acesso à internet geralmente é disponível, mas pode ser através de uma máquina ou rede não confiável. Um servidor proxy configurado corretamente pode permitir os usuários corretos no site enquanto bloqueia acesso para outros usuários.

O maior esforço atual em técnicas de firewall é encontrar uma combinação de um par de roteadores de filtragem com um ou mais servidores proxy na rede entre os dois roteadores. Esta configuração permite ao roteador externo bloquear qualquer tentativa de usar a camada IP subjacente para quebrar a segurança (IP spoofing, roteamento pela origem, fragmentos de pacotes), enquanto permite ao servidor proxy tratar potenciais furos de segurança nos protocolo das camadas superiores. A finalidade do roteador interno é bloquear todo tráfego exceto para o servidor proxy. Se esta configuração é implementada rigorosamente, pode ser obtido um alto nível de segurança.

Muitos firewalls fornecem capacidade de log que pode ser adequado para fazer administração mais conveniente da segurança da rede. A função de log pode ser centralizada e o sistema pode ser configurado para enviar alerta para condições anormais. É importante monitorar regularmente estes logs para qualquer sinal de intrusões ou tentativas de arrombamento. Desde que alguns intrusos tentarão encobrir seus ataques pela edição dos logs, é desejável proteger esses logs. Uma variedade de métodos está disponível, incluindo: escreva uma vez, leia muitos (WORM) drives; logs em papel; e logs centralizados através do utilitário "syslog". Outra técnica é usar uma impressora serial falsa, mas ter uma porta serial conectada para uma máquina isolada ou PC que mantêm os logs. Firewalls estão disponíveis em uma ampla faixa de qualidade e intensidade. Pacotes comerciais iniciam em aproximadamente $10.000 dólares e

alcançam mais de 250.000 dólares. Firewalls desenvolvidos pelo próprio site podem ser construídos para quantias menores de capital. Deve-se lembrar que a configuração correta de um firewall (comercial ou “caseiro”) requer uma significante habilidade e conhecimento do TCP/IP. Ambos os tipos requerem manutenção regular, instalação de patches de softwares e atualizações, e monitoração regular. Quando se realiza o orçamento de um firewall, estes custos adicionais deveriam ser considerados além do custo dos elementos físicos do firewall.

Como um aparte, construir uma solução caseira para um firewall requer significante habilidade e conhecimento do TCP/IP. Isto não deveria ser tentado trivialmente, pois a sensação de segurança percebida é pior ao longo da execução do que saber que não existe nenhuma segurança. Como com todas as medidas de segurança, é importante decidir na ameaça, o valor do recurso a ser protegido, e os custos para implementar segurança.

Uma nota final sobre firewalls. Eles podem ser uma grande ajuda quando implementando segurança para um site e protegem contra uma grande variedade de ataques. Mas é importante ter em mente que eles são apenas uma parte da solução. Eles não podem proteger seu site contra todos os tipos de ataque, é necessário ter outros mecanismo de segurança tais como: criptografia, antivírus, assinatura digital, autenticação e um bom projeto de segurança, para delinear, que informações devem ser protegidas, que posso deve ser dado em cada etapa do projeto.

CAPÍTULO 1

VISÃO GERAL DA SEGURANÇA EM INFORMÁTICA

1.1 - O AMBIENTE DE INFORMÁTICA E INFORMAÇÃO

1.1.1. - O valor da informação

Hoje, o bem mais valioso de uma empresa pode não estar sendo produzido por sua linha de produção ou não ser o serviço objeto de sua existência, como o serviço prestado por um banco (por exemplo). O bem mais valioso da empresa pode ser o conjunto de informações relacionadas com o bem que ela produz ou o serviço que presta a seus clientes.

Atualmente um banco não trabalha apenas com dinheiro, mas também com informações financeiras relacionadas com valores seus e de seus clientes. A maior parte desses dados é de natureza sigilosa, por força de determinação legal ou por se tratar de informação de natureza pessoal dos clientes ou informações que controlam e/ou demonstram a vida econômica dos clientes, que podem vir a sofrer danos caso sejam levadas a público.

Em uma empresa prestadora de serviços, em uma indústria ou no comércio, as informações são relacionadas com os seus processos de produção, políticas estratégicas, de marketing, cadastros de clientes etc. Não importa o meio físico em que residam, elas são de valor inestimável, não só para a empresa que as gerou, como para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria dos casos elas estão relacionadas com atividades diárias da empresa e sem elas poderia haver dificuldades.

Tradicionalmente, as empresa dedicam grande atenção à proteção de seus ativos físicos e financeiros, mas pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem; essa proteção tradicional pode nem visar a um bem valioso. Da mesma forma que seus ativos tangíveis, as informações envolvem os três fatores de produção tradicionais: capital, mão-de-obra e processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento físico - contábil que os outros ativos, do ponto de vista do negócio elas são um ativo da empresa e, portanto, devem ser protegidas.

Numa instituição financeira, o ambiente de informações não está restrito à área de informática, mas chega a mais longínqua localização geográfica onde a mesma tenha uma agência ou representação de qualquer tipo. Enquanto que na área de informática os ativos de informação são representados por dados armazenados, em sua maior parte residente em meios magnéticos, nas áreas fora do ambiente de informática esses ativos, representados em sua grande maioria por listagens ou microfichas, são muito mais tangíveis e de entendimento mais fácil por parte de seres humanos.

Não importa o meio físico em que residam informações; é importante ressaltar que muitas empresas não sobrevivem por mais de uns poucos dias a um colapso do fluxo de informações. E, dada à característica de tais empreendimentos - no caso de bancos essencialmente uma relação de confiança - é fácil prever que isso acarretaria completo descontrole sobre os negócios e até uma corrida ao caixa. E é fácil prever que a atual dependência das instituições financeiras em relação à informática se estenderá por toda a economia daqui para frente, tornando aos poucos todas as empresas altamente dependentes dos computadores e, consequentemente, cada vez mais sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle gerencial.

Os riscos são agravados de maneira geométrica à medida que informações essenciais ao gerenciamento dos negócios são centralizadas e principalmente com o grau de centralização. Ainda que esses riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob aspectos econômicos, quanto sob aspectos de agilização de processos de tomada de decisão em todos os níveis. Essa agilização é tanto mais necessária, quanto maior seja o uso de facilidades de processamento de informações pelos concorrentes. O que se precisa, antes de tudo, é cercar o ambiente de informações com medidas que garantam a sua segurança efetiva a um custo aceitável, visto ser impossível obter-se segurança absoluta, já que a partir de determinado nível os custos envolvidos com segurança tornam-se cada vez mais onerosos, superando os benefícios obtidos. Essas medidas devem estar claramente descritas na política global de segurança da organização, delineando as responsabilidades de cada grau da hierarquia, o grau de delegação de autoridade e, muito importante, claramente sustentadas pela alta direção da organização.

Segurança, mais que estrutura hierárquica, homens e equipamentos, é postura gerencial em uma organização, o que ultrapassa a tradicional abordagem dada à

segurança na maioria das empresas. Dado o caráter altamente dinâmico que as atividades relacionadas com o processamento de informações adquiriram ao longo do tempo, uma política de segurança de informações deve ser a mais ampla e mais simples possível. Por filosofia de segurança, entende-se política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras as mais claras e simples possíveis e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia. Deve ser delineada uma estrutura geral que não sofra as conseqüências das rápidas mutações que freqüentemente ocorrem com as atividades de processamento de informações, a política geral de segurança deve esboçar somente as regras básicas aplicáveis a toda a organização, deixando que cada área esboce as regras mais detalhadas que se relacionem com as suas próprias atividades, uma política de segurança deve, obrigatoriamente, contemplar os aspectos de classificação de ativos de informações quanto à sua proteção contra acessos não autorizados e sua preservação contra destruição. Além da proteção física e lógica, deve-se também contemplar o aspecto da recuperação da capacidade operacional, em casos de destruição parcial ou total da capacidade de processamento.

1.1.2 - A concepção de segurança

A segurança não é um produto acabado, ela reflete o agitado e dinâmico ambiente de empresa. Isto significa que não é verdade que uma vez implantada a segurança, as informações estarão seguras. Por outro lado, a implantação da segurança não é um processo simples, a estrutura de segurança deve refletir a estrutura organizacional da empresa da forma mais fiel possível, sob risco de causar transtornos ao fluxo de informações. A implantação da segurança deve ser um processo gradual. Grande parte, senão a maior parte, do esforço interno recai sobre os usuários dos sistemas de informação, pois nas áreas onde se desenvolvem as funções de negócios da empresa é que reside o conhecimento do que é importante para a empresa e, por isso, deve ser protegido, a segurança não é assunto de exclusiva responsabilidade da área de segurança. O conhecimento do que é importante para o negócio da empresa reside na área que é proprietária das informações e não na área de informática. Ainda que a área de informática seja uma das interessadas principais na segurança, é o proprietário das informações que deve avaliar o que deve ou não ser protegido e, dessa forma, a

segurança também passa a ser assunto de sua responsabilidade, a estrutura de segurança não é estática, pois reflete a estrutura dá empresa onde é implantada, precisa de constantes ajustes e mudanças para funcionar de maneira confiável, pois sofre o processo de envelhecimento normal a qualquer estrutura dinâmica.

1.1.3 - Riscos no ambiente de informática e informação

Os riscos no ambiente de informática e informação agravou-se após o aparecimento dos microcomputadores e a disseminação da cultura de informática em expressivos segmentos da sociedade, cada vez as organizações tornam-se dependentes de informações armazenadas em computadores; aproveita-se a grande velocidade e capacidade de cruzamento de informações que os computadores possuem, para se obter benefícios como rápida tomada de decisões, mudança rápida de estratégia, etc. Mas a mesma facilidade proporcionada pelos computadores também implica alto risco de violação, pois o mesmo programa usado para emitir um relatório de projeção de vendas, destinado ao diretor de marketing pode ser usado por um "espião" para emitir esse mesmo relatório para o diretor de marketing do concorrente. Dentre os riscos do ambiente de informática e informação, podemos observar que estão relacionadas naturalmente com a concentração das informações em um mesmo local ou máquina, as "invisibilidades" da informação gravadas nas diversas mídias, a concentração de funções de gestão de sistemas sobre poucos indivíduos, a falta de controles tornando impossíveis ações preventivas, a retenção de informação na mídia quando se elimina o arquivo que as contém, a possibilidade de cruzamento de informações revelando informações sigilosas, a possibilidade de introdução e propagação de erros, a possibilidade de acesso à informação por funcionários demissionários, a possibilidade de acessos não autorizados e suas mazelas (hackers, vírus, bombas lógicas, cavalos de tróia, alçapão, etc...). O furacão que arrastou grande parte das empresas brasileira para o comércio na Internet, no primeiro semestre de 2000, refletiu diretamente no mercado de tecnologia, gerando uma corrida por padrões de segurança da informação adequados ao novo cenário. Esse tema já figura entre as principais preocupações das empresas, mostrando-se cada vez mais estratégico para o resultado das companhias. A segurança virou um meio efetivo para viabilizar negócios já que o comercio eletrônico depende de confidencialidade e da confiabilidade, uma pesquisa realizada no

Brasil, no ultimo mês de setembro/2000 em diversos setores da indústria diz o seguinte: 34% dão prioridade máxima para a questão. Isso não quer dizer que tudo anda bem no reino da segurança. Assim como acontecia no modelo convencional de economia, pré-internet, parte das corporações ainda apresenta uma visão míope dos processos de proteção. É obvio que antes de se implantar qualquer infra-estrutura de segurança é necessário um estudo detalhado das necessidades e vulnerabilidade de cada ambiente, mas infelizmente as empresas tomam cominhos inversos. Segundo estudo realizado no Brasil, 35% das companhias não dispõe de meios para classificar as informações que necessitam de proteção em suas redes e, o pior 58 % das corporações não tem padrões regulares de revisão da política de segurança. A ansiedade de mercado digital pode ser apontada como a principal causa para essa inversão. As empresas tiveram de optar entre dois caminhos. Ou adiavam a entrada na Internet, para ganhar tempo de perceber as fragilidades do ambiente, e pagavam o preço de perderem posições no mercado. Ou encaravam o pioneirismo sob pena de errar pela falta de experiência e de exemplo a seguir. A partir do momento que as empresas decidiram conectarem-se suas redes privadas a Internet, o tema segurança tornou-se uma preocupação a mais. Os administradores de redes, por tudo isso, passam a ter crescentes preocupações a respeito da segurança de suas redes corporativas, quanto à invasão por parte de agentes externos (como *crackers*). Estatísticas apontam prejuízos de mais de cinco bilhões de dólares no período de 1997-1999, devidos a ataques de *hackers* e gangues cibernéticas.

1.2 – POLÍTICA DE SEGURANÇA

1.2.1 - Objetivos de uma política de segurança

Uma política de segurança de informação é um conjunto de diretrizes gerais com o fim de governar a proteção a ser dado à informação.

Seus objetivos podem ser:

- Reduzir a probabilidade de ocorrências;
- Reduzir os danos provocados por eventuais ocorrências;
- Criar procedimentos para se recuperar de eventuais danos.

As medidas de segurança devem ser, sempre que possível, de cunho preventivo. Os eventuais riscos devem ser eliminados antes que se manifestem. Pois, a prevenção

costuma sair mais barato que a restauração dos danos provocados por falta de segurança. De forma geral, as organizações conhecem os limites das atribuições e responsabilidades dentro de suas áreas de atuação e os riscos envolvidos, mesmo quando não há normas a respeito da segurança. As medidas de prevenção são, em princípio, principalmente de cunho normativo. As medidas para redução de danos provocados por eventuais ocorrências costumam ser de caráter normativo, pois em face da dinâmica de informática os procedimentos podem variar amplamente. Quanto aos procedimentos para se recuperar de eventuais danos, confunde-se com os procedimentos do plano de contingência a ser visto posteriormente.

1.2.2 - A cultura da empresa

Embora uma empresa deva estar aberta a mudanças ao longo de sua vida adaptando-se a novas situações, a introdução de novos controles e restrições sempre provocam resistência no ambiente da organização. A disseminação da cultura de informática contribuiu para a proliferação de "cursos de computação" de baixa qualidade o que resultou na redução da qualidade média da mão-de-obra oferecida no mercado. Além da menor competência profissional média do profissional de informática, há ainda o fato corriqueiro em administração de recursos humanos de se despedir mão-de-obra mais cara para contratar mão-de-obra mais barata. O profissional de informática trabalha com informações, produto intimamente relacionado com a cultura específica de cada empresa. A rotatividade de mão-de-obra nessa área implica um processo de aculturação do "novato" que dura algum tempo, durante o qual o custo dos erros freqüentemente ultrapassa os benefícios da redução da folha de pagamento, Além disso, mão-de-obra menos qualificada é menos propensa a seguir preceitos de segurança mais rígidos, dessa forma contribuindo para a disseminação de uma cultura de informática errada tanto do ponto de vista de segurança, como para os interesses das empresas e dos próprios profissionais. Tal perfil de profissional não permite a implantação de uma cultura de informática que vise à manutenção de um mínimo de segurança, visto que o ambiente cultural que formou essa mão-de-obra não tem preocupação com tais aspectos.

1.2.3 - A abrangência da política de segurança

Como já foi dito antes, segurança é uma questão de postura administrativa. Não se deve subestimar os aspectos técnicos envolvidos com a segurança, mas também evitar que a segurança fique presa a critérios meramente técnicos. A segurança em informática deve estar ligada a uma estrutura diretamente subordinada à alta administração, junto com as demais funções de controle, como auditoria, controladoria financeira e outras funções similares. Ainda que a segurança em informática envolva também aspectos clássicos da segurança, como vigilância, controle de acesso e outros controles similares, ela não deve ser encarada como uma extensão da tradicional segurança patrimonial, a política de segurança deve ter como área de abrangência no âmbito da organização, devendo-se definir claramente os ativos sobre os quais versará e o que se espera como proteção para cada tipo de ativo envolvido, como em qualquer atividade da organização, na elaboração da política de segurança, a primeira tarefa a ser realizada é a definição do que se deseja, fixando-se os objetivos a serem atendidos, definindo-se os meios e recursos necessários, estabelecendo-se as etapas a cumprir e os prazos das mesmas. A implantação da segurança deve seguir as mesmas etapas que seriam seguidas em qualquer outra atividade dentro da organização. Segurança também implica o uso de capital, mão-de-obra e recursos, isto é, representa investimento e despesas para a empresa. Nenhum administrador consciente pode se dar ao luxo de despender recursos materiais e financeiros sem que tenha um grau mínimo de certeza a respeito da atividade em que está aplicando esses recursos. As políticas de segurança devem apresentar diretrizes claras a respeito de, pelo menos, os seguintes aspectos.

- **Objetivo da segurança** – deve-se explicar de forma rápida e sucinta a finalidade da política de segurança;
- **A quem se destina** – definir claramente quais as estruturas organizacionais às quais a mesma se aplica;
- **Propriedade dos recursos** – deve-se definir, de forma clara, as regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações;
- **Responsabilidades** definir de forma clara qual o tipo de responsabilidades envolvidas com o manuseio de ativos de informações,

a quem as mesmas devem ser atribuídas e os mecanismos de transferência das mesmas;

- **Requisito de acesso –** deve-se indicar, de forma clara, quais os requisitos a serem atendidos para se poder acessar ativos de informações;
- **Generalidade –** deve-se definir aspectos que não cabem nas demais: definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias, etc.

1.2.4 - A educação em segurança

Uma política educacional com relação à segurança deve ser estabelecida na organização, antes da introdução de medidas de segurança. As pessoas envolvidas deverão estar conscientes e comprometidas com a política de segurança, o que deve estar em primeiro lugar nas preocupações de mesma. Cada funcionário novo admitido na organização deve receber treinamento sobre segurança, como parte do processo de ambientação do mesmo à cultura da organização. Esse treinamento inicial não precisa ser muito detalhado; o treinamento mais detalhado deve ser ministrado em cada área, em função das necessidades das mesmas. É recomendável ministrar treinamento periódico obrigatório.

1.2.5 - Aspectos da operacionalização

Uma vez identificada à necessidade de segurança e estabelecido o compromisso com a política de segurança da organização, já formalmente em vigor, a equipe de projeto passará à implantação de procedimentos. A seguir, deverá montar a estrutura de controle e administração da segurança.

CAPÍTULO 2

A SEGURANÇA DE ACESSO LÓGICO

2.1 - ASPECTOS GERAIS

2.1.1 - Acesso lógico

Desde o inicio da história da informática, sempre existiu alguma preocupação com a segurança física das instalações de informática. A segurança de acesso lógico, entretanto, é uma preocupação mais recente surgida principalmente em decorrência da proliferação de ambientes baseados em microcomputadores. Na realidade, a segurança de acesso lógico refere-se ao acesso que indivíduos passam ter a aplicações residentes dentro de ambientes informatizados, não importando assim o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são baseadas em software ou hardware, sendo, na maioria dos casos, “invisíveis” aos olhos das pessoas externas ao contexto. A segurança de acesso não é uma atividade que deva estar necessariamente na área de informática, pois está relacionada com as atividades de controle e auditoria da organização. O acesso lógico abrange aspectos como a execução de programas, funções e transações do ambiente informatizado bem como o acesso a bases de dados e, até mesmo, a utilização de computadores, outros equipamentos ou listagens tornando difícil dizer onde começa o acesso lógico e onde termina o acesso físico.

2.2 - A ADMINISTRAÇÃO DE SEGURANÇA

2.2.1 - A estrutura de administração de segurança

Na definição da estrutura de administração de segurança deve-se delinear cuidadosamente os aspectos: tipo de estrutura, a sua localização dentro da estrutura da organização, o perfil exigido do profissional que exercerá a função de administrador de segurança, as diretrizes da segurança, o ferramental administrativo e técnico a ser utilizado, a equipe de projeto incumbida de implementar a segurança, o grau de padronização e controle exigido, etc.

- **Tipa de estrutura - deve ser definida** o tipo de estrutura de administração da segurança, se centralizada ou descentralizada. Para ambos os tipos de

estrutura existem argumentos válidos, não havendo uma resposta pronta e certa para se tomar esse decisão. Pode haver uma resposta certa em relação a um ambiente individual, mas somente uma análise cuidadosa do ambiente de informações pode determinar qual será a resposta correta. A segurança **centralizada** proporciona controle mais eficiente com relação à mudança na segurança e possivelmente nos esforços para se impor à segurança. Mas o esforço de manutenção da segurança nesse nível pode requerer o gerenciamento de uma equipe considerável em tamanho e dedicação, a segurança **descentralizada** distribui o esforço de manutenção da segurança, de maneira que a função não se torne um ônus para qualquer área. Além disso, a manutenção poderá ser subordinado a uma área que pode ter um conhecimento maior e mais adequado dos recursos a serem protegidos. Entretanto, haverá um esforço adicional na área central para controlar as atividades dos administradores descentralizados. Muitas organizações começam com a administração centralizada e, posteriormente, descentralizam a função assim que os requisitos de manutenção tornem isso prático. Normalmente, essa é uma abordagem inicial mais racional, já que permite que a equipe do nível central se torne perita em segurança, antes que seja requisitada para treinar e controlar administradores e equipes em um nível descentralizado.

- **Localização da segurança** - a estrutura (ou função) de administração de segurança deve residir em algum lugar dentro da organização. Entretanto, o melhor lugar é onde a área de administração de segurança se relacione mais diretamente com a alta administração, em um dado ambiente de informações. Isso é necessário para que a área se torne menos suscetível a pressões e comprometimentos resultantes de lealdade para com a área funcional á qual a administração de segurança pertença. Também entendemos que pode ser vantajoso incluir todas as funções de segurança, compreendendo os requisitos de segurança física, dentro dessa área. A administração de segurança deve residir em uma área onde se necessário, ela tenha o poder de impor a segurança. Esse poder deve ser formalmente garantido e apoiado ativamente pela alta direção da empresa. A área deve ter também a mão-de-obra necessária para preencher as funções. Sob essas circunstâncias, a função de administração de segurança pode residir em qualquer lugar dentro da organização. É conveniente não ligar a administração de segurança a nenhuma das funções de informática, visto que elas também serão

consideradas como usuárias da segurança, nem à área de auditoria, pois cabe à mesma fiscalizar a área de segurança.

- **Perfil do administrador de segurança** - após a definição do posicionamento da administração de segurança, a próxima etapa é decidir quem irá preencher a função. O trabalho de um administrador de segurança é sem dúvida muito árduo. É uma posição de alta responsabilidade que requer uma forte personalidade, entre as diversas características que um administrador de segurança em potencial deve possuir, incluem-se:
    - Conhecimento dos recursos de informática e dos requisitos de segurança adequados aos mesmos;
    - Alto grau de responsabilidade;
    - Boa experiência analítica e organizacional;
    - Sensibilidade para a política do ambiente operacional;
    - Facilidade nos relacionamentos pessoais;
    - Estabilidade emocional.

É conveniente definir um substituto para o administrador de segurança desde o início, de maneira que a função possa continuar se, por qualquer motivo, o administrador de segurança inicialmente selecionado não o possa. Além do mais, pode ser necessária uma equipe de apoio, a equipe deve consistir de analistas de segurança e apoio administrativo, além do administrador de segurança.

Diz-se que “um bom administrador de segurança deve ter coração de pedra, nervos de aço e ser insensível a ofensas e insultos”**.**

- **Diretrizes da segurança** - o ideal é que as mesmas já estejam definidas na política global de segurança da empresa, como parte das atribuições e responsabilidades que se espera que todos os empregados sigam; as diretrizes de segurança mais específicas devem constar de normas à parte da política e devem basear-se nas diretrizes gerais da política, mas ainda assim não devem ser rígidas, para permitir adequação às particularidades de cada caso.

Por diretrizes, entendem-se as regras gerais que orientarão a elaboração de normas e procedimentos subordinados à política de segurança. Em princípio, as diretrizes de segurança devem contemplar os seguintes aspectos:

- Procedimento padrão de segurança que serão usados dentro do ambiente da empresa.
- Documentação dos controles de segurança disponíveis e sua comunicação a todos os envolvidos.
- Estimativa dos riscos e comprometimentos dentro do ambiente da empresa.
- Registro e relato das violações para as pessoas indicadas.
- Acompanhamento do desenvolvimento de requisitos de segurança para todos os projetos de usuários.
- Educação de todos os usuários com relação à política de segurança da empresa.
- Se for o caso, apoio às administrações descentralizadas e o seu controle.
- Responsabilização dos envolvidos com a função segurança, desde o administrador central até o usuário final; deve ser dada ênfase especial ao papel da área de informática em relação à segurança.
- Ferramental administrativo e técnico, o ferramental administrativo é altamente dependente da cultura de cada organização em particular. Já o ferramental técnico é dependente do produto de segurança adotado.
- Equipes do projeto, ao ser constituída a equipe de implantação do projeto, devem estar escritas às diretrizes que governarão o trabalho da equipe. O administrador de segurança, que já deve estar definido a esta altura, deve ser o coordenador da equipe, se a estrutura da administração de segurança já tiver sido implantada, é conveniente que pelo menos um dos integrantes da mesma participe da equipe, de preferência na função de relator e para providenciar os trâmites administrativos necessários.
- Padronização e controle, a padronização de nomenclatura é, por exemplo, o tipo de atividade que todos acham necessário, mas que, freqüentemente, vai sendo adiado indefinidamente. Se a organização conseguir desenvolver e impor padrões antes da implantação da segurança, ela será muito mais fácil, visto que os produtos de segurança são baseados, em grande parte, no agrupamento de funções de segurança proporcionado pela padronização.

Algumas atividades administrativas necessitam de controles firmes, e segurança em informática é uma delas. É necessários controlar o domínio de usuários, o domínio de recursos e as interações entre os dois domínios, a esta altura da montagem da estrutura de segurança, devem-se definir os controles desejados e que serão implantados após a escolha dos softwares de segurança. , todos os pacotes de segurança dispõem de recursos de emissão de relatório acerca da estrutura da segurança e das atividades dos usuários.

2.3 - SEGURANÇA EM MICROCOMPUTADORES

2.3.1 - Riscos envolvidos

Em todo o mundo a expansão da microinformática envolveu e continua a envolver pessoas com pouco ou nenhum contato anterior com computadores, ou seja, sem uma prévia cultura de informática, isso contribuiu para que os microcomputadores fossem tratados como mais um equipamento de escritório, que não exigia nenhuma medida especial de proteção. Além disso, o inicio dessa expansão ocorreu em princípios dos anos 80, época em que a segurança de informática ainda era uma preocupação maior apenas nos meios militares e governamentais. Ainda hoje, esse é o cenário predominante em microinformática, e isso implica riscos crescentes, na medida em que os microcomputadores aumentam de capacidade de processamento, com a conseqüente dependência de muitas organizações em relação aos mesmos, repetindo o processo ocorrido com os grandes computadores, de forma geral, os microcomputadores estão sujeitos aos mesmos riscos que os grandes computadores, acrescidos de alguns outros que são próprios dos ambientes de microinformática. A principal diferença reside na escala e no grau de acesso existente.

Os riscos envolvidos são decorrentes, principalmente, do acesso indiscriminado, ao contrário dos grandes computadores, onde o acesso físico é mais restrito, raramente os microcomputadores são objeto de um controle de acesso físico eficaz. É comum encontrar microcomputadores instalados em locais de grande circulação de pessoas e que abrigam sistemas de importância vital para a organização, sem dispor de controle de acesso através de software de segurança de acesso, recomenda-se que os microcomputadores sejam instalados em salas que possam ser trancadas quando fora de

uso, e que o acesso de pessoas a essas salas seja controlado, além disso, o acesso a microcomputadores deve ser feito através de chaves de acesso autenticadas por senhas, e controle sobre os domínios de recursos acessados, de modo a se poder auditar, e até por questões de apropriação de custos.

2.3.2 - Falta de controle

O Problema da falta de controles está intimamente associado com o problema do acesso indiscriminado, quanto maior o acesso a determinado ambiente, menor o controle existente, o controle de acesso, tanto físico quanto lógico, é fundamental para se coibir irregularidades em um ambiente informatizado, dessa forma, um novo cenário, a responsabilidade sobre a integridade das informações deixou de ser exclusiva do setor de segurança para tornar-se uma obrigação de todos os funcionários da companhia. Por outro lado, muitos usuários de microinformática acreditam ser os verdadeiros proprietários das aplicações que desenvolvem e, portanto, acham-se no direito de copiar e até vender as mesmas como se fossem suas, deve-se também lembrar que funcionários demissionários não devem, em hipótese alguma, continuar a ter acesso a facilidades computacionais da empresa. Em média, os levantamentos apontam que cerca de 70% dos problemas de segurança são gerados por falhas internas, quanto menos controle se exercer sobre um ambiente informatizado, maior o risco de acessos não autorizados. Isso é ainda mais sério em ambientes de microinformática do que entre grandes computadores, deve-se restringir o uso de recursos de microinformática para outras finalidades que não as relacionadas com os serviços a serem executados, dando atenção especial a jogos e ao uso de software pirata, para controlar o acesso indiscriminado, é aconselhável que além dos microcomputadores serem instalados em salas de acesso controlado, em cada disco rígido, instalar software de controle de acesso que permita a identificação dos usuários através do mecanismo de chaves de acesso autenticadas por senhas individuais. Fora de uso, mantenha essas salas trancadas a chaves e, se possível, desligue as linhas de energia que alimentam os microcomputadores instalados ali, devido à fragilidade dos controles de acesso em microinformática, deve-se dar atenção especial aos problemas relacionados com o uso de software não homologado pela organização. Além das implicações legais associadas com o direito autorais muitos softwares pirateados vêm “infectados” com vírus que podem provocar graves danos aos

ambientes de microinformática, e alguns deles podem ser até passados para ambientes de grandes computadores. Não existe nenhuma forma prática de se prevenir contra “vírus”, pois, da mesma forma que muitos de seus homônimos biológicos, os vírus de computadores possuem capacidade mutante e de rápida propagação dentro dos ambientes em que se instalam; normalmente, cada novo vírus exige uma forma de “vacina”.

2.3.3 - Vírus

Apesar de tratado à parte nesta seção, os “vírus” na realidade constituem-se em uma forma de acesso não autorizado tratada na seção anterior. Justifica-se o tratamento diferenciado devido às características assumidas atualmente pela “epidemia”. Até algum tempo ouvíamos falar de vírus do computador como coisa distante, poucos acreditavam que esse mal viesse a atacá-lo, hoje a realidade é outra, ainda assim, continua-se a acreditar que se trata de casos isolados. Em pouco tempo um verdadeiro surto fez com que os jornais e revistas estampassem muitas reportagens sobre o assunto. Desde as grandes empresas até as pequenas instalações, todos tinham histórias para contar (ou esconder) a respeito do tema, assim sendo, pode-se perceber, sem grande esforço, a quanto, anda a promiscuidade entre os mais diversos softwares circulando entre muitas máquinas. Tal como uma peste, a epidemia se alastra, bastando que um disquete contaminado seja acionado num micro são, vale a pena salientar que os vírus não atacam apenas microcomputadores, lembramos a contaminação da rede IBM a nível mundial, que ficou paralisada por algum tempo devido ao vírus da árvore de Natal. O mesmo se deu com a rede Internet nos EUA que sofreu uma infecção generalizada, causando um enorme prejuízo. Um vírus biológico costuma introduzir-se num organismo, apossando-se das células e obrigando-as a reproduzir milhares de cópias do vírus original. O vírus do computador, imitando o da natureza, atua de maneira semelhante: trata-se de um pequeno programa (conjunto de instruções) cujo objetivo, além de instalar-se, é reproduzir-se e dominar o organismo que o aloja.

O ciclo de vida dos vírus obedece às seguintes etapas:

- **Criação** - alguém escreve um programa que tem por objetivo inserir-se em outros programas, proliferando-se e executando as tarefas a que está programado num dado momento.

- **Disseminação** - muitas vezes o vírus fica agregado a um software que se torna seu “cavalo de Tróia”. Ele se propaga toda vez que o dono do “cavalo de Tróia” troca software com outras pessoas por meio de redes públicas ou disquetes.

- **Contágio** - quanto mais o programa hospedeiro se propaga, mais o vírus se reproduz e logo estará difundido. Muitas vezes não se percebe a infecção, uma vez que o vírus foi programado para ficar em estado latente por muito tempo.

- **Ataque** - numa época predeterminada, o vírus desperta. O sinal vem do próprio relógio/calendário interno que os computadores usam para controlar seu processamento, o vírus assume o controle da máquina e começam os estragos, os vírus continuam sendo os grandes vilões dos profissionais de segurança, respondendo por 73% dos problemas ocorridos nos último ano, e em grande parte são disseminados pelos próprios funcionários.

2.3.4 - Programas antivírus ou vacinas

Os melhores programas deste tipo são os que evitam a instalação do vírus, as principais características deste tipo de programa são:

- Não aceita mudar arquivos de execução.
- Não deixa qualquer programa ficar residente sem autorização do usuário.
- Não permite que se rode um programa que não esteja numa lista de aplicações previamente testada e aprovada.

O problema é que a cada novo vírus deverá ser criado um novo programa detector, o agravante é que os vírus conhecidos, a exemplo dos seus similares biológicos, têm capacidade de mutação e estão sofrendo pequenas modificações, o que dificulta sua identificação por meio de comparações de códigos e o seu combate, e, da mesma forma, adquirem resistência aos “antibióticos”, assim sendo, o melhor é o tratamento preventivo.

2.3.5 - Recomendações para evitar a contaminação

Dentre as medidas preventivas que podem ser adotadas para evitar a contaminação por vírus, recomendamos:

- Evitar programas de origem desconhecida (cópias piratas);
- Utilizar programas originais ou reproduções de procedência oficial;

- Restringir o acesso de operadores não autorizados, por meio de softwares de segurança;
- Caso receba software em demonstração, deixe-os isolados num único micro;
- Evite utilizar os comandos DEL ou ERASE para limpar disquetes, dê preferência ao FORMAT;
- Não permitir acesso aos micros por pessoas desconhecidas ou funcionários demissionários;
- Procure manter a sala onde estão os equipamentos fechados à chave;
- Caso empreste disquetes, faça uma cópia antes e formate-os se recebê-los de volta, ou não os receba de volta;
- Não utilizar o micro para jogos trazidos de fora, cuja procedência seja impossível de verificar;
- Manter sempre uma cópia de segurança das informações, de acordo com o ciclo de atualização;
- Se houver necessidade de reinstalar software utilize os disquetes originais;
- Evite a troca indiscriminada de disquetes;
- Colocar banda de proteção (write-protect) contra gravação nos disquetes que contenham programas ou que não necessitem ser gravado.

CAPÍTULO 3

A SEGURANÇA FÍSICA

3.1 - ASPECTOS GERAIS

3.1.1 - Introdução

Embora o ambiente de comunicação de dados, especialmente o de redes em comunicação via Internet, tenha aumentado a preocupação com segurança lógica, restringindo acessos e protegendo dados, um plano de segurança jamais seria completo se não fossem observados, preliminarmente, os aspectos de segurança física. A sobrevivência de uma empresa informatizada está ligada á operacionalidade de seus centros de informática em alguns casos ainda chamados de CPD's. Em tais pontos costumam estarem concentrados servidores, equipamentos de rede (switches, hubs, roteadores,...), nobreaks, etc. Assim, a primeira linha de defesa contra eventuais desastres é um plano de segurança física. O plano de segurança física, entretanto, não é suficiente para garantir a segurança contra todas as possibilidades de ocorrências, o que leva à necessidade de uma segunda linha de defesa contra desastres, um plano de recuperação, ou plano de contingência, temos, assim, dois aspectos da segurança física:

- Preventivo - plano de segurança física;
- Contingencial - plano de contingência.

Quando as medidas preventivas de segurança falham, ou são incapazes de evitar uma ocorrência catastrófica para o centro de informática, deve possuir soluções previstas ou preparadas previamente para a adoção rápida de medidas de emergência a fim de garantir a sobrevivência da empresa após o desastre, ou seja, o plano de contingência, também chamado plano de recuperação de desastres.

3.1.2 - Objetivos principais da segurança física

Dentre os objetivos principais da segurança física em informática, deve-se destacar os pontos abaixo:

- Manter a integridade e confidencialidade das informações;
- Garantir a continuidade da atividade de informática na empresa;

- Garantir a integridade dos ativos da empresa controlados pelos sistemas computadorizados.

3.2 - RECOMENDAÇÕES PARA PROJETOS DE SEGURANÇA FÍSICA

3.2.1 - Quanto à localização e arquitetura

A construção de um centro de informática deve observar, tanto quanto possível, os seguintes requisitos quanto à localização e elementos de arquitetura:

- Localização - evitar locais sujeitos à inundação interferência de radiofreqüência, interferência eletromagnética, vibrações ou impactos de alta intensidade e alto nível de poluição atmosférica.
- Arquitetura - observar necessidade de:
  - Expansão futura;
  - Local adequado para instalação de nobreaks e banco de baterias;
  - Área para instalação de grupo-gerador diesel e tanques de combustível;
  - Proteção contra eventual inundação;
  - Divisórios tetos e painéis de acabamento retardantes ao fogo;
  - Acessos com dimensões que possibilitem a entrada e saída de equipamentos;
  - Sinalização dos acessos;
  - Iluminação (não incandescente) evitando reflexos nas telas de monitores, interferências (RFI) de reatores e transientes elétricos, que venham afetar o funcionamento dos computadores.

3.2.2 - Quanto à infra-estrutura

Recomenda-se observar os seguintes requisitos de infra-estrutura:

- Rede Elétrica - a rede elétrica para computadores e periféricos da empresa deve ser independente, ou seja, deve ter quadros de distribuição e circuitos exclusivos para esses equipamentos. Por outro lado não deve existir computadores ou periféricos ligados na rede de iluminação geral da empresa;

- Energia Elétrica - deve haver fonte alternativa de energia apoiada em nobreaks e grupo-gerador com partida automática, garantindo ininterruptamente energia elétrica de boa qualidade;
- Segurança contra fogo - deve haver alarmes de acionamento automático, revisados periodicamente. Além disso, o pessoal operacional deve ser treinado (e reciclado) com testes periódicos de uso dos equipamentos disponíveis no combate ao fogo.
- Climatização - A temperatura e umidade devem ser mantidas nos padrões exigidos para funcionamento dos equipamentos, sendo indispensável;
  - Utilização de um sistema central exclusivo para cento de informática;
  - Redundância de equipamentos e dispositivos;
  - Utilização de sensores nos dispositivos de controle de temperatura e Umidade relativa;
  - Previsão de sistemas adequados e eficientes de filtragem e vedação;
  - Utilização de sistemas de ar condicionado que independam de água para seu funcionamento.

O controle de temperatura e umidade relativa deve ser mantido segundo parâmetros do fabricante dos equipamentos. São as seguintes às características gerais desses parâmetros:

- Temperatura ideal de 22ºC, com tolerância de ±10ºC;
- Umidade relativa ideal de 50% com tolerância de ± 5%;
- Variação máxima de temperatura de 1ºC/5 minutos;
- Variação máxima de umidade relativa de 45% a 55% em menos de oito Horas.

3.3 - CONTROLE DE ACESSO FÍSICO

3.3.1 - Sistemas de controle

Os sistemas de controle aqui têm por objetivo a segurança de acesso a áreas delimitadas, edifícios, salas de computadores e de arquivos, centrais de instalações e equipamentos auxiliares, Cada tipo de empresa deve aqui avaliar o grau de risco a que estão expostas quanto a seus dados, equipamentos e recursos.

Recomenda-se que esta avaliação seja feita levando em conta o nível de impacto que é representado pelas conseqüências trazidas para a empresa, em função de perda, furto, destruição, alteração ou divulgação de recursos de hardware, software, infra-estruturas e informações. Avaliado o grau de risco a que a empresa está exposta, é chegado o momento de optar pelos sistemas de controle de acesso, que basicamente podem ser:

- Sistemas automáticos - são sistemas que atuam independentemente das ações humanas, geralmente controladas por computadores acoplados a dispositivos ou sensores eletrônicos. Além de dar apoio a medidas corretivas, esse tipo de sistema pode também efetuar procedimentos automaticamente, tais como acionamento de alarmes, ligações telefônicas a locais programados, travamento ou liberação de portas e acessos, registro automático de entrada e saídas, etc. Ex: Monitoração por circuito fechado de TV sensoriamento interno ininterrupto com ligação ou alarma para a central de segurança, etc.

- Sistemas semi-automáticos - são sistemas que obrigatoriamente dependem de interação humana para seu funcionamento. Geralmente são compostos de dispositivos acionados elétrica ou mecanicamente, controlados por um atendente que libera ou não o acesso, dependendo de as condições terem sido satisfeitas. EX: interfones, porteiros eletrônicos, etc.

- Sistemas simples - são sistemas que geralmente utilizam apenas supervisão humana (através de porteiros, vigilantes ou funcionários da própria área). Fisicamente, esses locais podem ser protegidos por restrições de acesso físico convencionais, tais como portas comuns e fechaduras. Em alguns casos pode ser necessário o registro do visitante, que geralmente é preenchido ou anotado pelo atendente. Podem ser adotados também crachás especiais que autorizam o acesso do portador.

3.3.2 - Áreas de risco e requisitos de segurança

No que se refere as controle de acesso físico as áreas de risco devem ser identificadas e mapeadas sobre a planta do prédio, para que se estabeleçam os requisitos e medidas de segurança. As áreas do centro de informática e adjacências devem ser

divididas em zonas concêntricas de segurança baseadas na “teoria da cebola”, onde à parte mais protegida deve ser a parte central.

O acesso aos quadros de controle de equipamentos auxiliares bem como caixa de passagem de cabos de eletricidade e de telecomunicações deve ser limitado por chaves, Os seguintes tipos de quadros, mesmo que situados na sala do computador, devem ser mantidos fechados permanentemente, exceto por ocasião de reparos ou limpeza:

- Quadros de controle de equipamentos;
- Quadros de telefones e caixas de terminais;
- Quadros de energia elétrica, painéis de distribuição, dispositivos de controle de corrente, medidores de demanda, interruptores manuais e interruptores gerais;

Para aumentar o nível de segurança de quadros de controle e caixas de passagem, recomenda-se a utilização de sensoriamento, a entrada de objetos estranhos à sala de computadores deve sofrer restrições. De modo geral, deve ser proibidas a entrada de pessoas portando bolsas, pacotes, malas etc., devendo esses objetos ser deixados fora do ambiente, a não ser que sejam estritamente necessários e que se sujeitem à revista. Os itens abaixo devem ser proibidos em qualquer ocasião:

- Ímãs ou qualquer aparelho que gere campo magnético;
- Equipamento eletroeletrônico de uso pessoal;
- Copiadores de documentos e câmeras em geral;
- Alimentos e bebidas;
- Qualquer material de fumantes;
- Material radioativo, tóxico, produtos químicos, explosivos ou outros materiais que possam representar risco à instalação ou às pessoas que nela trabalham.

A central deverá supervisionar seus circuitos de alarme quanto a falhas para terra, curto-circuito ou interrupção. Os comandos de operação da central deverão ser bloqueados eletronicamente e liberados por senha. Deverá haver, associado à central, um repetidor de alarme localizado na sala de segurança da empresa. Os sinais de alarme deverão ser diferenciados acústica e visualmente dos sinais de defeito. Os circuitos de alarme, em caso de defeito, não deverão impedir o funcionamento dos outros circuitos.

A alimentação elétrica deverá prever alimentação de emergência adequada que possa prevenir do fornecimento normal.

3.4 - SEGURANÇA CONTRA FOGO

3.4.1 - Aspectos preventivos

Os aspectos preventivos da segurança contra fogo são estabelecidos na sua maior parte no momento do projeto de arquitetura e infra-estrutura. Seus requisitos e conceitos estão claramente especificados por normas da ABNT e já foram mencionados no item oito. Tratam basicamente de:

- Material de divisórias, tetos, mobiliaria e utensílios (cesto de papéis, por exemplo);
- Tipo de luminárias;
- Bitola e especificação correta de cabos e dispositivos elétricos;
- Isolamento com relação a eventuais áreas de risco da empresa.

3.4.2 - Detecção de fogo

Existe uma infinidade métodos de detecção de incêndio, mas, nos centros de processamento de dados ou centrais de informática, os sistemas baseados na produção de fumaça ou combustão de gás são os mais eficientes. Para que um sistema de detecção seja considerado eficiente, deve atender, no mínimo, aos seguintes requisitos:

Acionar os alarmes numa primeira instância quando qualquer elemento sensor (detector) detectar fumaça ou gás de combustão, e acionar o sistema de combate quando um segundo elemento sensível acusar a detecção.

- Controlar os ventiladores e os dispositivos de fechamento no sistema de condicionamento de ar.
- Cortar ou não a alimentação da eletricidade para o equipamento, de acordo com o desejo do utilizador, que deverá julgar se o prejuízo causado pelo corte da corrente para o equipamento é ou não compensador.
- Operar alarmes perceptíveis em pontos estratégicos, tais como o próprio recinto ou escritório do responsável pelo local ou vigilante de plantão.

Todos os tipos de avisos devem ser monitorados em local específico na área de informática. Avisos importantes (alarmes) devem ser retransmitidos para a sala de segurança geral do prédio, ou outro local com vigilância permanente.

Os painéis devem estar preparados para funcionar com energia própria (sistema de energia ininterrupto) e avisar falhas. Painéis mais sofisticados devem ter dois ou mais níveis de alarme e saídas (digitais e/ou analógicas), para interligações.

Quanto ao tipo de detectores a serem usados no centro de informática, o ideal é haver uma intercalação de detectores de fumaça do tipo iônico e do tipo óptico, numa concentração de um detector para cada 15m. Os detectores térmicos normalmente não têm aplicação visto que o seu grau de sensibilidade somente permite detectar um incêndio quando o mesmo já tiver causado grandes estragos, principalmente em função da fumaça. Entretanto, podem ser utilizados em recintos destinados aos equipamentos de infra-estrutura e de apoio, como a casa das máquinas (grupo-gerador e ar condicionado central) e a sala de baterias.

3.4.3 - Extinção de fogo

Em local onde a água não pode ser usada (subestações elétricas, equipamento eletroeletrônico etc.), são instalados sistemas á base de gás. Os agentes extintores usados são o CO2 (mais comum) e o halon 1301.

A decisão acerca do uso de um sistema automático de detecção e combate a incêndios depende de várias condições de operação e poderá ser tomado pela análise principalmente, do tempo de uso diário das instalações, o extintor portátil de dióxido de carbono (CO2), de operação manual, devem ser disseminados pelo recinto do centro de informática, e no mínimo um aparelho deve estar disponível na entrada da sala. Todos os aparelhos devem estar marcados de forma visível e em local de fácil acesso, extintores de espuma e pó químico não devem ser usados, equipamento de combate a incêndio usando água como agente extintor não deverá ser usado no recinto do centro de informática, mas sim estar do lado de fora da área, para combater os incêndios que não envolvam o equipamento de processamento de dados, embora capazes de virem a afetá-lo indiretamente. Deve ter o decalque “NÃO USE EM ELETRICIDADE”.

Para concluir é necessário que a ação a ser seguida em caso de incêndio seja do conhecimento de todos no que se refere a procedimentos a serem adotados.

3.5 - AMBIENTE DE OPERAÇÃO E ARMAZENAMENTO

3.5.1 - Requisitos mínimos de climatização

O objetivo das recomendações aqui apresentadas é facilitar a tarefa de proporcionar a todos os tipos de mídias de armazenamento de dados, a segurança cabível. Essas recomendações abrangem os limites de temperatura, umidade, poluição e campo magnético no ambiente de arquivamento operação, ou transporte, existem no mercado equipamentos munidos de sensores com a finalidade de manter cada um dos fatores mencionados dentro dos limites ideais para operação, armazenamento e transporte que, de um modo geral, são os seguintes (para discos rígidos, disquetes, fitas, discos ópticos):

- Temperatura
  - Mínima: 17ºC.
  - Máxima: 23ºC.
  - Variação máxima ±2ºC por hora.
  - Limite de emergência: 75ºC.
- Umidade relativa
  - Mínima: 45%.
  - Máxima: 55%.
  - Variação máxima: 5% por 24 horas.
  - Limite de emergência: 85%.
- Poluição (Nº máximo de partículas no ar por m^3)
  - Menor que 5 µm: até 30.000
  - Maior que 5 µm: isento.

Embora os limites acima sejam os ideais, eventualmente os fatores em questão podem oscilar numa faixa mais larga:

- Temperatura
  - Mínima: + 5ºC.
  - Máxima: + 32ºC.
- Unidade relativa
  - Mínima: 20%.

- Máxima: 60%.

- Poluição (Nº máximo de partículas no ar por m^3)

  - Menor que 5 μ m: até oito milhões.

  - Maior que 5 μ m: até 25.000.

O projeto de condicionamento de ar com os respectivos dutos deve ser feito tendo em vista evitar a difusão de fogo e de fumaça. Para tanto, devem ser satisfeitas as seguintes exigências mínimas:

- Instalação de condicionamento de ar para o centro de informática, independente e exclusiva.
- Pressão de ar positiva dentro do recinto.
- Uso de filtros incombustíveis.
- Não devem ser usados materiais combustíveis na rede de dutos, no isolamento térmico e no tratamento acústico.
- Controle para desligar os ventiladores, no caso de início de incêndio no recinto.
- Instalação para extrair fumaça do recinto.

Controles manuais localizados fora do recinto, para alcançar os objetivos indicados nos dois últimos itens. Recomenda-se que, ao se pesquisar os equipamentos necessários, sejam exigidos do fornecedor laudo de laboratório independente, demonstrando que eles foram testados conforme as normas internacionais, ou seja, numa condição que simule uma situação real. Campos magnéticos de 4000Å/metro são fatais para mídias magnéticas. Entretanto, a 10mm de distância é necessário uma corrente de 250A para a atingir esse valor. Mesmo assim recomendam-se distâncias de segurança bem maiores, já que raios e outros transientes podem causar picos muitos altos com efeitos graves, apesar da duração de milionésimos de segundo**.** Emissoras de ondas de rádio e principalmente de radar merecem cuidados especiais, mesmo a distâncias variando entre um e dois km, as proibições de fumar, tomar café, fazer refeições e outras regras de comportamento são óbvias, mas deve ser rigorosamente implementada em todo lugar onde existir mídia magnética.

3.5.2 - Ambiente de armazenamento e transporte

O armazenamento de mídias magnéticas ou ópticas pode exigir a construção de salas ou cofres de segurança com características especiais para manutenção dos requisitos de climatização estabelecidos no item anterior. As salas de segurança devem r utilizar tanto para proteger os arquivos de dados, como para abrigar, por exemplo, equipamentos de comunicação de dados (hubs, switches, roteadores, etc) ou instalações de hardware que não necessitem de intervenção de operadores (discos fixos e CPUS).

O transporte deve ser feito em cofres portáteis, que só devem ser abertos na sala de operação ou local que assegure os requisitos de climatização.

3.6 - SEGURANÇA PARA ESTAÇÃO DE TRABALHO

3.6.1 - Equipamentos e mídias locais

As medidas de segurança a serem desenvolvidas e implementadas para estações de trabalho e mídias dependem, basicamente, do grau de dependência que seu uso representa para a continuidade dos negócios ou atividades da empresa. Quanto mais dependentes as empresa se tornarem dos recursos de informática, mais deve ser investido em segurança.

Assim, podemos avaliar cada caso da seguinte maneira:

- Alto risco (impacto total) - impede a continuidade do negócio.
- Risco intermediário (impacto parcial) - impõe algumas dificuldades ao negócio.
- Baixo risco (nenhum impacto) - não afeta o negócio.

Baseados nesses níveis, as organizações e usuários devem classificar-se para então justificar as medidas de proteção adequadas para cada caso.

Assim sendo, tudo o que foi mencionado anteriormente pode ser aplicado para estações de trabalho e mídias locais dependendo do grau de proteção desejado.

3.6.2 - O aspecto administrativo

Devem ser mantidas, em local seguro, pastas com a documentação de seus serviços, que deverão conter, no mínimo, os seguintes itens:

- Aplicação ou serviço;

- Programas utilizados;
- Documentação dos programas utilizados. Fórmulas no caso de planilhas;
- Definição dos arquivos utilizados, no caso de programas de gerenciamento de arquivos em banco de dados;
- Disquetes utilizados;
- Nomes de programas e arquivos. Devem ser criados padrões e nomes de arquivos e de programas, procurando facilitar a rápida identificação dos trabalhos desenvolvidos.

3.6.3 - Cópias de segurança

É aconselhável que cada setor tenha, além das cópias de segurança locais em disquete, uma cópia a mais no cofre ou sala de segurança da empresa.

CAPÍTULO 4

A SEGURANÇA NA INTERNET

4.1 - A VULNERABILIDADE DA INTERNET

4.1.1 - Ameaças à segurança

O uso da Internet pode dar como retorno ganho de produtividade e economia de custo, na medida em que oferece o acesso às informações externas e a interligação entre pontos remotos da empresa. Entretanto, para obter esses benefícios, as empresas devem expor suas redes a ameaças potencialmente sérias. Para que possa se certificar de que seu patrimônio está seguro, uma empresa deve compreender essas ameaças e tomar as providências necessárias para proteger informações, recursos e redes. Este item discute os principais tipos de ameaças e aspectos vulneráveis que as empresas enfrentam ao optar pelo uso da Internet e apresenta uma introdução aos controles de segurança que podem ser usados para conter essas ameaças. As ameaças vêm tanto da Internet quanto de redes internas, mas não na mesma proporção. Significativamente, há mais ameaças por parte das redes internas de uma empresa - de 80 a 95 por cento do número total de incidentes de segurança (de acordo com diversos estudos)**.** Com isso, obviamente, apenas um pequeno percentual de ameaças realmente tem origem na própria Internet. O nível de segurança da sua rede interna é de importância primordial. Tudo o que dissermos sobre como criar um firewall seguro ou sobre como garantir a segurança de serviços comerciais ou de serviços destinados ao usuário final não significa relaxar a segurança dos sistemas internos. É necessário um programa de segurança global efetivo para garantir uma proteção adequada. As propriedades intrínsecas da Internet representam a principal fonte de sua vulnerabilidade a falhas e ataques. A Internet conecta centenas de redes espalhadas pelo mundo inteiro, seu enorme tamanho afeta sua confiabilidade e abre uma porta para inúmeros problemas em um grande número de pontos, tais como:

Roteamentos incorretos, falhas de transmissão e falhas de componentes físicos (como roteadores), são pontos fracos da tecnologia - os hackers têm total conhecimento de determinados pontos vulneráveis dos sistemas, na verdade com freqüência, o fornecedor ou o hacker divulga a existência de um bug de sistema ou de um furo na

segurança depois que o problema é descoberto. Organizações como a CERT (Computer Emergency Response Team) divulgam pontos vulneráveis (e correções); jornais informativos destacam os feitos dos hackers, geralmente, as fraquezas tecnológicas podem ser classificadas em duas categorias: as causadas por deficiência inerentes a mecanismos e produtos, e as que resultam da configuração incorreta de sistemas operacionais e de programas aplicativos, muitos desses problemas podem ser resultantes de deficiências nos protocolos de comunicação. Os protocolos definem o conjunto de regras em que se baseia a interoperação das redes. Muitos protocolos são usados juntamente com outros e agregados em “conjuntos de protocolos”. Muitos protocolos têm características inatas que os tornam vulneráveis a ataques. O TCP/IP, por exemplo, sofre de problemas congênitos.

Dentre esses problemas, o principal é sua inabilidade para confirmar a identidade dos participantes em um processo de comunicação. Sob o TCP/IP, qualquer computador pode criar mensagens que parecem ter uma outra origem. Para isso, basta criar mensagens falsas que contêm endereços para “devolução” também falsos. Outra deficiência importante é sua inabilidade de proteger a privacidade dos dados de uma rede. Uma determinada máquina pode monitorar todo o tráfego de uma rede a que está conectada, independente de seu destino. O sistema operacional UNIX, por exemplo, é muito utilizado hoje em dia juntamente com o conjunto de protocolos TCP/IP. Mas como o UNIX foi originalmente projetado para compartilhar informações sem qualquer restrição, a maior parte dos sistemas UNIX apresenta algum tipo de ponto vulnerável, quando você compra um sistema operacional UNIX, normalmente ele contém um arquivo de “confiança” que contém uma lista de hosts (ou computadores) que o seu sistema reconhece. Esses hosts são considerados como “confiáveis”; isso significa que um login remoto talvez não precise de uma senha. Em outras palavras, se o host B estiver listado no arquivo de confiança de A, uma pessoa (que tem uma conta no Host A e no B) poderá estabelecer um logon com o Host A partir do Host B sem fornecer uma senha. Alguns sistemas são distribuídos sem um sinal de adição (+) em seu arquivo de confiança, indicando que todos os hosts da Internet são considerados como confiáveis. Se uma conta tiver o mesmo nome nos dois sistemas, não será necessária uma senha para que haja o logon com o sistema confiável.

A computação colaborativa requer o freqüente compartilhamento de recursos, o que, obviamente, torna o uso do arquivo de confiança ainda mais interessante, mas não elimina o risco de segurança. A forma como esse arquivo é utilizada - caso o seja - passa a ser uma questão de política de segurança. Se permitir que os desenvolvedores (ou qualquer outra pessoa) utilizem o acesso confiável, você deverá compreender a fundo as ameaças, configurar o arquivo de forma a minimizar o risco e aplicar controles de compensação, como a monitoração e o log de sistema, algumas empresas conectam apenas um host isolado à Internet, mas muitas outras conectam centenas de máquinas. A conectividade também varia - algumas empresas têm conexões dedicadas de alta velocidade com a Internet, enquanto outras mantêm linhas simples de discagem por modem. A possibilidade de a Internet acomodar tal diversidade é vantajosa, mas também cria muitos pontos vulneráveis que podem ser difíceis de controlar. Quando foi projetada inicialmente, o objetivo da Internet era permitir diversas possibilidades de conectividade entre partes que estivessem interagindo. Portanto, a interoperabilidade, e não a segurança, foi enfatizada. Apesar de essa característica ter sido aceita quando a Internet era principalmente uma rede de pesquisa, com a demanda comercial cada vez maior, a falta de serviços de segurança passou a ser pedra no caminho de sua utilização comercial, deve-se estar sempre protegido contra muitas ameaças ao se estabelecer conexão com a Internet, mas elas podem ser generalizadas em algumas categorias mais comuns.

- Ameaças à Rede Corporativa - A disponibilidade de serviços da Internet pode abrir furos na segurança que permitem o acesso de intrusos a outros componentes da rede de computadores.
- Ameaças aos Servidores da Internet - Intrusos podem entrar em um servidor da Internet (digamos um servidor da WWW); com isso, eles têm a possibilidade de ler ou até mesmo modificar arquivos armazenados no servidor. Um comerciante que armazena números de cartão de crédito em um servidor conectado à Internet corre o risco de passar por muitos problemas.
- Ameaças à Transmissão de Dados - A confidencialidade e a integridade das informações podem ser violadas se alguém interceptar a comunicação

com a rede da empresa (correio eletrônico, transações da Web, downloads de arquivos etc.).

- Ameaças à Disponibilidade dos Serviços - Um intruso mal-intencionado poderia perpetrar um ataque que interromperia a disponibilidade de sistemas, ou até mesmo da rede inteira, para seus legítimos usuários.
- Ameaças de Repudiação - Um participante de uma transação online pode negar que a transação realmente tenha acontecido.

4.1.2 - Pontos fracos

As ameaças exploram sempre pontos fracos de um sistema, geralmente relacionados à tecnologia ou à política de operação. As fraquezas tecnológicas que se referem a deficiências nos produtos de software e hardware que se utilizam e as falhas no material de comunicação. As fraquezas na política de operação se referem às regras pelas quais operamos sistemas de computador. O projeto de um sistema seguro é tão importante quanto ter uma política de segurança eficiente. A ameaça só é eliminada quando os dois estão presentes.

- Pontos fracos da tecnologia - um ponto fraco com origem na tecnologia decorre do fato de que muitos sistemas operacionais são complexos e de difícil configuração. Além disso, são fornecidos com parâmetros básicos que inerentemente não são seguros (tais como o parâmetro básico + no arquivo de confiança do UNIX). Outros exemplos de pontos fracos na configuração de sistemas são os seguintes:
    - Contas do usuário inseguras (como logins de convidados ou contas de usuários expiradas);
    - Contas de sistema com senhas originais muito conhecidas que não são alteradas;
    - Serviços da Internet incorretamente configurados;
    - Parâmetros básicos inseguros nos produtos.

Uma forma de ajudar o tratamento desses pontos fracos é utilizar recursos de segurança e auditoria nos sistemas para detectar os problemas assim que eles surgirem. Antes de comprar um aplicativo ou produto, avalie seus recursos de segurança e de auditoria. Caso ele não ofereça o nível de segurança que você deseja, não o compre ou certifique-se de que existe um produto para complementá-lo, ou verifique se há

controles de compensação disponíveis. Os produtos podem ter excelentes recursos de segurança, mas se não estiverem ativados, não oferecerão qualquer proteção. Recursos incorretamente configurados também podem resultar em uma deficiência em termos de segurança.

- Pontos fracos da política de operação - a política de operação geralmente abrange os seguintes controles básicos:
  - Controles de acesso físico;
  - Controles de acesso lógico;
  - Administração de segurança;
  - Monitoração e auditoria de segurança;
  - Gerenciamento de modificações em software e hardware;
  - Backup e recuperação de desastre;
  - Continuidade dos negócios.

Cada um desses controles deve ser implementado de forma consistente, em toda a empresa. Nenhuma ligação fraca deve permanecer. Esses controles básicos são essenciais para ajudar a proteger a rede das ameaças baseadas na Internet (e ameaças internas também). Todavia, nenhuma solução deve ser considerada como capaz de oferecer toda a proteção necessária. Os pontos fracos também podem surgir a partir de diretrizes corporativas inadequadas relacionadas a práticas e procedimentos de segurança. Por exemplo, com freqüência, os usuários escolhem senhas que podem ser descobertas com facilidade, por simples ignorância do que isso pode acarretar. A existência de uma política sólida para uso de senhas pode representar um grande caminho a ser percorrido para corrigir esse comportamento. A falha na especificação desses controles pode acarretar problemas na estratégia de segurança da empresa que deixarão as redes e sistemas extremamente vulneráveis a ataques.

4.1.3 - O invasor

Durante anos, os profissionais da área de segurança de informações e a comunidade que impõe leis têm tentado identificar quem são exatamente os invasores de redes, denominados “hackers” ou, mais apropriadamente, “crackers”. O projeto Slammer, conduzido pela Agência de Segurança Nacional dos Estados Unidos, pelo Serviço de Investigação da Força Aérea e pelo FBI, tentou identificar as características

psicológicas dos crackers entrevistando inúmeras pessoas que haviam sido sentenciadas por crimes decorrentes do mau uso do computador. Os investigadores encontraram um fato em comum: geralmente os crackers são pessoas solitárias que vivem isoladas dos outros. No entanto, esse estudo foi criticado porque a amostra continha apenas pessoas que realmente haviam sido condenadas por crimes envolvendo o mau uso do computador. Portanto, talvez as amostras não representem corretamente a comunidade de crackers - isso sem falar naqueles cuja habilidade impediu que sua ação fosse detectada.

O SRI International promoveu um estado semelhante em 1993. Ao entrevistar vários crackers assumidos, os investigadores concluíram que as características mais comuns entre eles eram as decepções, as grandes desilusões (geralmente reveladas através de seus apelidos, que denotavam poder e destruição, como Dark Avenger e Doutor Doom) e o desajuste social, obviamente identificar o invasor é uma operação onerosa, mas importante. Identificar muitos dos inúmeros motivos que levam algumas pessoas a atacar sistemas de computador parece ser uma estratégia mais interessante. Crackers assumidos revelaram os seguintes motivos para seus atos.

Ganhos financeiros - Com freqüência, os intrusos são funcionários que obtêm acesso a sistemas financeiros para roubar dinheiro (através da transferência eletrônica de fundos, por exemplo). Geralmente, esses funcionários ganham menos do que outros que estão o mesmo tempo na empresa. Devido à conectividade (à Internet) cada vez maior das redes corporativas e a medidas de controle de segurança ineficazes, crackers atraídos pela promessa de ganhos financeiros têm obtido acesso remoto não-autorizado a sistemas que processam transações de clientes, a bancos de dados financeiros etc. Esses violadores transferem fundos para eles mesmos ou reduzem o valor devido a alguém, vingança - outro importante motivação para entradas não-autorizadas em sistemas e redes é a vingança de funcionários. O risco de atividades não-autorizadas envolvendo o uso de computadores aumenta substancialmente quando funcionários são dispensados, demitidos, rebaixados, preteridos em promoções ou em sua percepção, mal pagos ou tratados de forma injusta. O não-cancelamento do acesso remoto de funcionários desligados a servidores, sistemas e a outros recursos computacionais acaba criando um canal conveniente para os motivados por vingança. Os estudos de caso

sugerem que a vingança é mais provável de resultar em problemas ou danos a sistemas do que a maioria dos outros motivos.

Necessidade de aceitação ou Respeito - muitos intrusos se dedicam a atividades ilegais envolvendo o uso do computador devido à necessidade de aceitação e/ou respeito de outras pessoas, e não por cobiça ou vingança. Com freqüência, membros de clubes de hackers ganham aceitação ao cometerem atos como violar a conta de alguém muito famoso e acessar entradas de um diretório que contém informações pessoais (como um histórico profissional), idealismo - alguns intrusos atacam sistemas por razões idealistas. Eles se vêem como heróis protegendo o mundo de operações clandestinas de coleta de dados por parte do governo. Outros afirmam que estão encontrando pontos vulneráveis para tornar as redes e os sistemas mais seguros, anarquia - os anarquistas penetram nos sistemas simplesmente para produzir a discórdia e a segregação. Esses “phreakers” e “cyberpunks”, que é a forma como são chamados, são motivados pela emoção provocada pelo desenvolvimento de atividades não-autorizadas, aprendizados - uma pequena parte daqueles que violam sistemas faz isso para aprender mais sobre hacking.

Curiosidade ou busca de emoção - outro motivo muito comum para a intrusão em sistemas é a curiosidade. Alguns intrusos simplesmente querem saber “o que existe naquele sistema”, espionagem industrial - a espionagem industrial ocorre quando uma empresa ou organização se dedica a atividades ilegais contra outra empresa ou organização, ignorância - alguns intrusos não têm consciência de que suas ações são ilegais e podem ser punidos, espionagem nacional - a espionagem nacional é semelhante à espionagem industrial, exceto pelo fato de que um país ataca os recursos de informática de outro. O termo “guerra da informação”, que é usado com freqüência, não se limita à área da espionagem nacional. Um segredo não muito bem disfarçado foi o que aconteceu durante a operação Tempestade no Deserto. Nesse evento, o Iraque recebeu informações sobre o movimento das tropas dos Estados Unidos; intrusos europeus acessaram remotamente computadores militares dos Estados Unidos e transferiram grandes volumes de informação que foram vendidas posteriormente.

4.1.4 - Tipos de ataques

Dentre os muitos tipos de ataques já registrados na Internet, merecem destaque os seguintes:

Ataques baseados em senhas - o invasor, de posse do nome do usuário e "possíveis" senhas, tenta o acesso, informando uma combinação de nome do usuário/senha, depois outra e assim por diante, até que uma determinada combinação permita sua entrada no sistema. Essa estratégia da força bruta tem sucesso em muitos tipos de sistemas UNIX que não bloqueiam tentativas de login após um determinado número de insucessos. Essa fraqueza inerente em termos de segurança permite a um intruso dar início a um grande número de tentativas de login que não são impedidas.

Às vezes, os violadores descobrem as senhas das seguintes formas: acessando mensagens de correio eletrônico que contêm senhas; ou decifrando-as com uma ferramenta que permita localizar e obter informações sobre senhas vulneráveis em sistemas UNIX. Alguns crackers utilizam TFTP ou FTP para tentar obter de forma remota o arquivo de senhas (etc/passwd) em sistemas UNIX. As senhas contidas em etc/passwd são criptografadas através de um esquema de criptografia não-convencional, mas o algoritmo de criptografia em si está largamente disponível e pode ser até mesmo incorporado em algumas ferramentas utilizadas pelos crackers. Os crackers as utilizam para obter senhas em textos simples que serão informadas durante sessões de telnet ou de rlogin. Com freqüência, a obtenção de senhas e a perpetração de ataques de força bruta consomem um volume considerável de tempo e esforço. Portanto, muitos crackers abandonaram os ataques baseados em senhas para obter acesso não-autorizado a sistemas remotos através da Internet. Vários sistemas operacionais (incluindo UNIX, VMS e Windows NT) têm mecanismos de acesso confiável projetados para facilitar o acesso a outros sistemas e domínios. No que se refere aos sistemas conectados à Internet, os mecanismos de acesso confiável são muito mais explorados em sistemas UNIX do que em qualquer outra plataforma. Os sistemas UNIX permitem o uso de arquivos de host confiáveis (como os arquivos hosts dos diretórios home) formados por nomes de hosts e/ou endereços a partir dos quais um usuário pode obter acesso sem utilizar uma senha. O usuário deve simplesmente executar o comando rlogin, ou outros semelhantes, utilizando os argumentos apropriados. O violador que adivinhar o nome de uma máquina ou de uma combinação host/nome do usuário poderá acessar uma máquina que permita acesso confiável. Com freqüência, os administradores do sistema definem arquivos hosts no diretório-raiz para permitir que eles se desloquem rapidamente de um host para outro com privilégios-raiz (de superusuário). Um violador

que adivinhe corretamente a existência de tal acesso confiável entre hosts poderá obter facilmente um acesso-raiz não-autorizado. Além disso, como mencionamos anteriormente, a presença da entrada + (ou alguns sistemas UNIX, ++) no arquivo etc/hosts.Equiv pode permitir um acesso confiável a qualquer pessoa que tente executar um rlogin com um host UNIX. O pior ainda é que na maioria dos sistemas UNIX o arquivo /etc/hosts.Equiv permite o acesso a qualquer identificador de usuário (UID) de um sistema, exceto à raiz (UID=0). Essa característica permite que uma pessoa que não está definida como usuária de um sistema UNIX estabeleça login com qualquer número de contas de usuário. A ameaça do acesso confiável não-autorizado a hosts aumenta ainda mais quando existe uma "simetria de confiança" ou uma confiança mútua entre dois hosts. Um violador só precisa obter acesso a uma máquina para que possa acessar a outra. A "transitividade de confiança", uma condição na qual o acesso confiável de uma primeira máquina para outra e desta para uma terceira permite o acesso confiável da primeira para a terceira máquina, também impõe altos níveis de risco de segurança. Restringir (ou em alguns casos, proibir) a simetria de confiança e a transitividade de confiança reduz substancialmente os riscos de segurança na Internet.

Ataques baseados em spoofing do IP - o spoofing do IP apoia-se no fornecimento de informações falsas sobre a identidade de um host (ou pessoa) para obter acesso não autorizado. A primeira etapa de um ataque de spoofing é identificar duas máquinas de destino, que chamaremos de A e B. Na maioria dos casos, uma máquina terá um relacionamento confiável com a outra. É esse relacionamento que o ataque de spoofing tentará explorar. Uma vez que os sistemas de destino tenham sido identificados, o violador tentará estabelecer uma conexão com a máquina B de forma que B acredite que tem uma conexão com A, quando na realidade a conexão é com a máquina do violador, que chamaremos de X. Isso é feito através da criação de uma mensagem falsa (uma mensagem criada na máquina X, mas que contém o endereço de origem de A) solicitando uma conexão com B. Mediante o recebimento dessa mensagem, B responderá com uma mensagem semelhante que reconhece a solicitação e estabelece números de seqüência.

Sob circunstâncias normais, essa mensagem de B seria combinada a uma terceira mensagem reconhecendo o número de seqüência de B. Com isso, o "handshake" seria concluído, e a conexão poderia prosseguir. No entanto, como acredita que está se

comunicando com A, B envia sua resposta a A, e não para X. Com isso, X terá de responder a B sem conhecer os números de seqüência gerados por B. Portanto, X deverá adivinhar com precisão os números de seqüência que B utilizará. Em determinadas situações, isso é mais fácil do que se possa imaginar, No entanto, além de adivinhar o número de seqüência, o violador deverá impedir que a mensagem de B chegue até A. Se a mensagem tivesse de chegar a A, A negaria ter solicitado uma conexão, e o ataque de spoofing falharia. Para alcanças esse objetivo, normalmente o intruso enviaria diversos pacotes à máquina A para esgotar sua capacidade e impedir que ela respondesse à mensagem de B. Essa técnica é conhecida como “violação de portas”. Uma vez que essa operação tenha chegado ao fim, o violador poderá concluir a falsa conexão. O spoofing do IP, no seu passo-a-passo, é uma estratégia desajeitada e entediante. No entanto, uma análise recente revelou a existência de ferramentas capazes de executar um ataque de spoofing em menos de 20 segundos. O spoofing do IP é uma ameaça perigosa, cada vez maior, mas, por sorte, é relativamente fácil criar mecanismos de proteção contra ela. A melhor defesa contra o spoofing é configurar roteadores de modo a rejeitar qualquer pacote recebido cuja origem alegada seja um host da rede interna. Essa simples precaução impedirá que qualquer máquina externa tire vantagem de relacionamentos confiáveis dentro da rede interna. No entanto, essa medida não tratará de relacionamentos que ultrapassam os limites da rede.

Ataques baseados em seqüestro de sessão - mesmo com o uso de ferramentas automatizadas, os ataques baseados em spoofing não são fáceis de executar. Exigem a previsão de números de seqüência desconhecidos e permitem apenas uma conexão em uma só via com uma rede - portanto, os intrusos podem enviar mensagens para uma rede, mas não podem recebê-las (eventuais respostas serão enviadas ao host genuíno, A, conforme exemplo anterior). Os ataques de spoofing seriam mais comuns e problemáticos caso os intrusos não tivessem essas restrições. Na verdade, essas situações existem e são chamadas de “segurança” de sessão. O seqüestro (ou roubo) de sessão é semelhante ao spoofing do IP; na verdade, algumas pessoas o consideram como um tipo especial de spoofing do IP. No seqüestro de sessão, um intruso procura por uma conexão já existente entre dois hosts e tenta ter o controle sobre ela. Após obter o controle da máquina (um firewall ou um componente da rede de um provedor de serviços) através da qual a conexão é estabelecida, ou de outra máquina da mesma

LAN, o intruso monitora a conexão que está sendo efetuada. Dessa forma, o intruso é capaz de determinar os números de seqüência utilizados por ambos os lados da conexão sem o complicado processo descrito anteriormente. Após ver a conexão, o intruso pode gerar um tráfego que parece vir de um dos dois hosts, simplesmente "roubando" a sessão de uma das duas pessoas envolvidas no processo. Ao fazê-lo, o intruso obtém os mesmos privilégios de acesso que o usuário legítimo. Em conseqüência disso, o usuário legítimo é descartado da conexão, e o intruso pode continuar o que o usuário original havia começado. A proteção contra seqüestro de sessão é extremamente difícil. Até mesmo os mecanismos de autenticação mais rígidos nem sempre tem êxito ao impedir ataques de seqüestro. Apesar de a existência de uma proteção adequada para roteadores e firewalls contra o acesso não-autorizado (por exemplo, removendo contas padrão desnecessárias e corrigindo características vulneráveis relacionadas à segurança) poder reduzir enormemente a possibilidade desses ataques, a única real defesa contra esses ataques é o intenso uso de criptografia.

Ataques baseados em monitoramento - uma rede de meios físicos compartilhados é uma rede na qual os pacotes são transmitidos de todas as partes da rede, à medida que trafegam dos pontos de origem para os de destino. As redes de meios físicos compartilhados impõem um tipo especial de risco de segurança, pois os pacotes podem ser interceptados em qualquer ponto dessas redes a menos que medidas de controle especiais sejam adotadas. A captura de pacotes dessa forma é conhecida como rastreamento da rede (ou, alternativamente, como rastreamento de pacotes ou monitoração promíscua). Como é principalmente uma rede de meios físicos compartilhados, a Internet está vulnerável a esse tipo de ingerência. Na verdade, nos últimos anos, ocorreram centenas de milhares de ataques à Internet nos quais pacotes de login foram capturados. Os intrusos examinavam esses pacotes para determinar o nome do host, o nome do usuário e a senha, e utilizavam o telnet para estabelecer login com sistemas sem que lhes fosse dada autorização. Se um "farejador" for instalado em alguma parte da rota entre um host de origem e um host de destino instalados na rede de uma empresa, as informações de login poderão ser capturadas e posteriormente usadas para atacar o host de destino. Essa situação ocorreu várias vezes; em 1993 e 1994, farejadores de pacotes foram largamente instalados em redes nas quais havia roteadores que eram utilizados por provedores de serviços regionais. Todos os pacotes de login que

chegavam a esses roteadores eram capturados; os primeiros 128 bytes de cada pacote (contendo informações de login) eram descarregados em um arquivo aparentemente inócuo que os violadores acessavam e liam periodicamente. O rastreamento da rede é uma das mais sérias ameaças a empresas, mesmo que suas redes não se conectem a Internet. Esse método de ataque é útil para que intrusos não apenas capturem informações de login, mas também obtenham ilegalmente dados e mensagens eletrônicas de uma empresa. Além disso, a proteção contra atos de ingerência na rede normalmente não é tão fácil quanto parece, como explicaremos a seguir.

Ataques baseados na vulnerabilidade da tecnologia - os crackers exploram diariamente os pontos vulneráveis existentes em sistemas operacionais e seus programas de serviços (Sendmail, FTP, NFS, NIS, etc). Esses pontos vulneráveis podem ser explorados para permitir inúmeras ações não-autorizadas, incluindo o uso desses serviços, o acesso a sistemas de arquivos de importância crítica (e sua possível modificação), o acesso a dados do usuário e/ou programas (e sua possível modificação) e privilégios de acesso. Com freqüência, os fornecedores corrigem esses pontos vulneráveis, apenas para descobrir que algum outro usuário de Internet (incluindo alguém da comunidade de crackers) encontrou uma outra forma de comprometer um ou mais desses serviços e que, portanto, será necessária uma outra correção. O problema fundamental é que muitos programas de serviço TCP/IP apresentam falhas relativas à segurança. Ninguém parece estar disposto a reescrevê-los completamente; portanto, vários patches, um após o outro, são criados para tratar do “ponto vulnerável da semana” descrito na CERT e em relatórios do fornecedor. É aconselháveis corrigir aspectos tecnológicos vulneráveis de importância crítica - aqueles com maiores possibilidades de prejudicar processos comerciais ou de comprometer dados fundamentais.

4.1.5 - O que fazer

Para se defender das muitas ameaças à segurança, a empresa deve estabelecer controles de segurança que serão usados como base para um programa de segurança de informações. Dentre os princípios de segurança de informações geralmente aceitos estão a proteção da confidencialidade, da integridade e da disponibilidade - uma combinação conhecida no mundo da informação como CID (ou CIA, em inglês). Confidencialidade

significa proteger as informações contra sua revelação para alguém não-autorizado - interna ou externamente. A integridade se refere à proteção dos dados contra perda, modificação ou danos - deliberados ou não. A disponibilidade diz respeito à necessidade de se ter às informações acessíveis e prontas para uso, o que representa um objetivo crítico para qualquer empresa que se baseie no processamento em computadores. Sem sistemas de segurança que utilizem esses controles, a empresa não pode ter garantia de que os seus dados são confiáveis, esses três controles básicos podem ser complementados com outros para proporcionar mais segurança. A ISO (International Standards Organization) define um padrão que inclui outros controles como autenticação, controle de acesso e não-repudiação, para determinar quem é o usuário, a empresa deverá ter um controle de identificação e autenticação, antes de conceder acesso a qualquer sistema corporativo. Em muitos casos, talvez sejam necessários muitos níveis de identificação e autenticação. Para obter acesso à rede da empresa, talvez seja preciso um logon. Talvez haja necessidade também de um segundo logon em nível de aplicação, por exemplo, para abrir um sistema financeiro ou de correio eletrônico. Em muitos casos, um terceiro logon pode ser necessário em nível de transação para sistemas financeiros que tratem de atividades comerciais. A identificação e a autenticação são extremamente importantes para confirmar a identidade do usuário. Muitas pessoas as consideram como a base para todos os outros controles de segurança.

Uma vez que os usuários tenham sido autenticados, o controle de acesso estabelecerá quais direitos e privilégios serão atribuídos a eles. Esse importante controle garante que os usuários sejam autorizados a executar suas responsabilidades e fiquem limitados a elas, e não recebam direitos de acesso que excedam suas necessidades. O controle de auditoria, também deve ser incluído porque fornece um registro não só do uso de recursos do sistema, como também das ações por parte do usuário. Trilhas de auditoria adequadas permitem que as empresas façam análises de diagnóstico e de violação. O controle de não-repudiação está se tornando cada vez mais importante à medida que o uso do comércio eletrônico se consagra. Serviços comerciais estão sendo controlados eletronicamente. Para que as transações eletrônicas sejam legais, as duas partes devem reconhecer uma a outra e devem ser autorizadas a fazer a transação. Além disso, a origem e o destino da transação devem ser conhecidos por ambas às partes e

devem ser válidos para impedir a ocorrência de contestações referentes à posse ou ao recebimento de serviços.

4.2 - CRIPTOGRAFIA

4.2.1 - Visão geral

A criptografia é a medida lógica de defesa mais factível e prática para proteção da informação. A criptografia é baseada num mecanismo de conversão (o algoritmo de cifragem) para converter as informações de texto claro para texto cifrado, através do uso de uma chave de cifragem somente do conhecimento do emitente e do receptor (em princípio); o mecanismo pode ser até de conhecimento público, mas as chaves usadas no processo nunca podem ser reveladas e, devido ao risco de decifração do texto e conseqüente dedução da chave, as mesmas devem ser trocadas com freqüência, o que implica a possibilidade de interceptação do meio usado para comunicar as chaves entre as partes, as técnicas criptográficas são baseadas na substituição e/ou na transposição de caracteres (ou bits). A substituição consiste na troca de determinado padrão de caracteres ou bits por outro padrão estabelecido pela chave de cifragem. A transposição implica a troca de posição das seqüências dentro da mensagem, controlada pela chave. Em ambos os processos, pode haver diversas passagens pelo algoritmo de cifragem antes que a mensagem seja transmitida. Na outra ponta da linha, o processo inverso é executado e se obtém de volta o texto original, a criptografia exige uma série de procedimentos de segurança, a maioria dos quais de caráter administrativo. A criptografia é conhecida desde a mais remota antiguidade, quando era usada principalmente para comunicações militares. Foi somente neste século que o seu uso em transações comercias tornou-se mais amplo. A criptografia pode ser usada em comunicação de dados, para proteger dados sensíveis contra revelação, principalmente as transações de transferência de fundos entre bancos.

Tradicionalmente, o processo de criptografia implica a existência de um algoritmo criptográfico que, através uma chave de cifragem, transforma um texto claro em criptograma. Isso implica o conhecimento do algoritmo de cifragem por parte de ambos os envolvidos no processo, ou mesmo o uso de um algoritmo de conhecimento público, e da chave de cifragem/decifração. As chaves usadas no processo precisam ser

transmitidas pelo emissor para o receptor. Devido ao risco quebra da cifragem através de análise do criptograma, existe a possibilidade de um determinado criptograma vir a ser decifrado e revelar o algoritmo e a chave usada para cifrar. Por esse motivo, as chaves de cifragem são trocadas freqüentemente, de acordo com um esquema combinado previamente. É nesse ponto que reside à vulnerabilidade do processo; a forma de comunicar as chaves usadas no processo é passível de interceptação por terceiros. Além do risco de interceptação, a lista de chaves precisa ser arquivada em algum meio de registro, e isso também é passível de revelação.

4.2.2 - Criptografia de chave simétrica

Apesar de os computadores terem mudado o campo da criptografia, seus princípios fundamentais permaneceram os mesmos; as mensagens eram codificadas com uma chave secreta ou compartilhadas e eram decodificadas com a mesma chave. Esse método, conhecido como criptografia tradicional ou criptografia com chave simétrica, funciona bem em aplicações limitadas, como as militares, onde o emissor e o receptor podem se preparar antecipadamente para trocar a chave. Infelizmente, genericamente esse método não funciona muito bem, pois trocar chaves secretas com todas as pessoas a quem você queira enviar uma mensagem é praticamente impossível. Para ilustrar isso, considere o que teríamos de fazer se tivéssemos de enviar um memorando confidencial para acionistas de uma empresa. Primeiro teríamos de entrar em contado com cada acionista individualmente para que pudesse fazer a troca das chaves secretas. Isso poderia ser feito ao telefone, mas se as mensagens fossem extremamente confidenciais, talvez fosse melhor trocar chaves por correio eletrônico ou até mesmo pessoalmente. Lembre-se de que precisaríamos fazer isso para todas as pessoas; cada uma teria uma chave secreta separada. Para aumentar a complexidade desse sistema, também deveríamos lembrar de qual chave serve para cada cliente. Se misturá-las, os clientes não serão capazes de ler as suas mensagens. Obviamente, esse tipo de sistema não é viável para transações comerciais comuns.

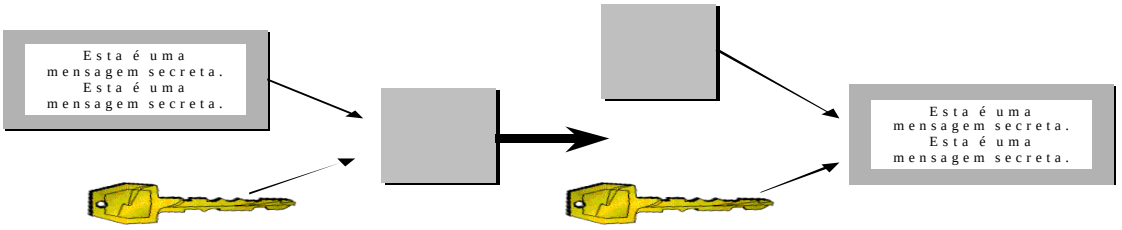

Figura 1 – *Como funciona a criptografia de chave simétrica.*

Os algoritmos de chave simétrica mais usados são:

DES (Data Encryption Standard) - uma cifragem de bloco criada pela IBM e endossada pelo governo dos Estados Unidos em 1977. O DES utiliza uma chave de 56 bits e opera em blocos de 64 bits. Projetado para ser implementado em componentes de hardware, ele é relativamente rápido e é usados com freqüência para criptografar grandes volumes de dados de uma só vez. O DES é usado em muitas das aplicações mais seguras da Internet, incluindo a SSL (Secure Sockets Layer) e a maioria das alternativas mais seguras do IP. O DES poderia ter seu uso mais difundido, mas as leis dos Estados Unidos restringem sua exportação. Durante a RSA conference´99, cinco mil pessoas de todo o mundo discutiam o presente e o futuro do uso da criptografia. Alguns números, sintetizados pelo Criptographi Center of Excellence da Princewaterhouse Coopers, sediada em New York, EUA, apresentam a evolução dos esforços empregados na quebra do DES, algoritmo usado até então pelo governo americano, em vias de ser substituído:

- 1997, janeiro – cinco meses, combinando capacidade computacional via internet.
- 1998, janeiro – 39 dias, usando recursos semelhantes.
- 1998, julho – 56 horas, usando uma única máquina da EFF, organização que realiza estudos sobre a internet.
- 1999, janeiro 22 ¼ horas, pelos mesmos meios e pessoas anteriores.

DES Triplo - um documento publicado recentemente descreveu uma “máquina de um milhão de dólares” que seria capaz de violar chaves DES rapidamente. Como o projeto dessa máquina só caberia no orçamento de governos federais e de grandes corporações, muitas pessoas e pequenas empresas começaram a endossar o uso do DES

triplo, no qual um bloco de dados é criptografado três vezes com diferentes chaves, como uma alternativa ao DES.

RC2 e RC4 - Ron Rivest, da RSADSI (RSA Data Security Inc.), projetou as cifras RC2 e RC4 com tamanho de chave variável para proporcionar uma criptografia em alto volume que fosse muito rápida. Um pouco mais rápidas do que o DES, essas cifras podem se tornar mais seguras escolhendo-se um tamanho de chave mais longo. O RC2 pode servir muito bem como um substituto para o DES, pois ambos são cifras de bloco. O RC4 é um outro tipo de cifra conhecida como cifra de fluxo. Em software, o RC2 é aproximadamente duas vezes mais rápido do que o DES, ao passo que o RC4 é 10 vezes mais rápido que o DES, vantagem - a grande vantagem do RC2 e do RC4 é que eles são exportados com muito mais facilidade pelos Estados Unidos do que DES, em parte por causa de uma transação que a Software Publishers Association fechou com o governo dos Estados Unidos, o que tornou a exportação do RC2 e do RC4 muito mais fácil com chaves de 40 bits. Os algoritmos RC são as cifras mais usadas para os softwares exportados pelos Estados Unidos. IDEA (International Data Encryption Algorithm) - esse relativamente novo algoritmo de criptografia foi criado em 1991. Ele foi projetado para ser facilmente calculado em softwares, é muito forte e é resistente a muitas formas de criptoanálise.

4.2.3 - Criptografia de chave assimétrica

Na década de 1970 foi inventadas a criptografia de chave assimétrica ou criptografia com chave pública, onde uma chave é usada para criptografar uma mensagem e outra é usada para decriptografar a mesma mensagem, em um sistema de chave pública, cada pessoa tem duas chaves: uma chave pública e uma chave privada. As mensagens criptografadas com uma das chaves do par só podem ser decriptografadas com a outra chave correspondente; portanto, qualquer mensagem criptografada com a chave privada só pode ser decriptografada pela chave pública e vice-versa. Como o nome sugere, normalmente a chave pública é mantida universalmente disponível. A outra chave, a chave privada, é mantida em segredo. Apesar das muitas tentativas de criar um criptossistema de chave pública totalmente funcional, até agora apenas um superou o teste do tempo e uma vigilância rígida. Conhecida simplesmente como RSA, esse sistema teve seu nome inspirado em seus três desenvolvedores, Ron Rivest, Adi

Shamir e Leonard Adleman. A RSADSI (RSA Data Security Incorporated) tem e defende vigorosamente a patente do RSA nos Estados Unidos, através de um exemplo, ilustraremos como a criptografia com chave pública funciona. Se Eduardo e Mônica quiserem se comunicar secretamente usando a criptografia com chave pública, eles terão de fazer o seguinte:

- **1º)** Eduardo escreve uma mensagem e a criptografa utilizando a chave pública de Mônica. A chave pública está disponível para qualquer pessoa.
- **2º)** Eduardo envia a mensagem para Mônica através da Internet.
- **3º)** Mônica recebe a mensagem e a decriptografa utilizando sua chave privada.
- **4º)** Mônica lê a mensagem. Se quiser responder, ela devera fazer o mesmo, a diferença é que dessa vez a chave pública de Eduardo será utilizada.

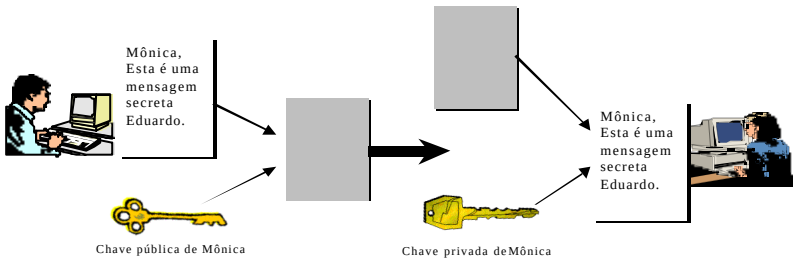

Figura 2 – *Como funciona a criptografia de chave assimétrica.*

Como apenas Mônica tem acesso à sua própria chave privada (pressupondo-se que a segurança do sistema seja eficiente), somente ela poderá ler a mensagem, pois existe confidencialidade. A grande vantagem desse sistema é que não só Eduardo pode enviar mensagens secretas a Mônica - todo mundo pode. Tudo o que o emissor precisa é da chave pública dela, é importante enfatizar nesse momento que o sigilo da chave privada é importantíssimo, o criptossistema inteiro se baseia no fato de que a chave privada é realmente privada. Se um invasor conseguir roubar a sua chave privada, tudo estará perdido. Não importa qual seja a eficiência do algoritmo de criptografia - o intruso vencerá e poderá ler e criar mensagens utilizando seu nome.

4.2.4 - Assinatura digital

A possibilidade de ter chaves pública e privada (separadas) proporciona outro benefício: a **assinatura digital**. Imagine como seria usar o sistema de forma invertida. Em vez de Eduardo criptografar a mensagem com a chave pública de Mônica, ele utiliza sua própria chave privada. Agora todo mundo pode ler a mensagem; ela deixou de ser secreta. Isso é verdade, mas também é verdade que apenas Eduardo poderia ter escrito a mensagem. Ele é única pessoa capaz de criar mensagens que possam ser lida com sua chave pública, pressupondo-se, obviamente, que Eduardo não tenha compartilhado sua chave privada com ninguém mais e que ela seja realmente secreta.

Um exemplo esclarecerá melhor o que estamos falando. Eduardo agora quer enviar uma mensagem para todos os seus contatos informando-os que mudaram de emprego. Na verdade, ele não se importa com quem lerá a mensagem, mas quer ter certeza de garantir a seus contatos de que a mensagem realmente é dele, e não outra pessoa. A seqüência a seguir atinge esse objetivo:

- **1º)** Eduardo escreve a mensagem e a criptografa utilizando sua chave privada.
- **2º)** Eduardo envia a mensagem a seus contatos através da Internet.
- **3º)** Os contatos recebem a mensagem e a decriptografa utilizando a chave pública de Eduardo.

O fato de a chave pública de Eduardo ter decriptografado a mensagem garante aos contatos que a mensagem realmente é de Eduardo. Qualquer mensagem decriptografada com a chave pública de Eduardo só poderia ter sido criada com sua chave privada. Isso é **muito importante**. Na criptografia com chave pública, cada par de chaves é única. Só existe uma chave pública para cada chave privada e vice-versa. Se isso não fosse verdade, a assinatura digital não seria possível; um impostor poderia utilizar outra chave privada para criar uma mensagem que pudesse ser lida pela chave pública fornecida, a assinatura digital implementa os objetivos de segurança da **integridade e da não-repudiação** apresentados no **item 1.5**. Como acabamos de ver, a **assinatura digital** assegura aos contatos que a mensagem não foi alterada (integridade) e que ela veio de Eduardo (autenticidade). Além disso, Eduardo não pode negar que tenha enviado a mensagem (não-repudiação), pois é o único com acesso a sua chave privada. Agora, o que acontecerá se Eduardo enviar uma mensagem privada

assinada a Mônica. Tudo o que Eduardo precisa é combinar os dois métodos, da forma mostrada a seguir:

- **(1º)** Eduardo escreve a mensagem e a criptografa utilizando sua chave privada (ele assina a mensagem).
- **(2º)** Em seguida, ele decriptografa a mensagem com a chave pública de Mônica (tornando-a privada).
- **(3º)** Eduardo envia a mensagem duplamente criptografada para Mônica através da Internet.
- **(4º)** Mônica recebe a mensagem.
- **(5º)** Ela decriptografa a mensagem duas vezes. Primeiro, ela utiliza sua chave privada e, depois, a chave pública de Eduardo. Observe que ela está invertendo os passos que Eduardo executou para criar a mensagem.
- **(6º)** Mônica agora pode ler a mensagem e tem certeza de que ela é secreta e veio de Eduardo. Ela também tem certeza de que a mensagem não foi modificada; para alterá-la, o invasor teria de acessar a chave privada de Eduardo.

4.2.5 - Combinando criptografias simétrica e assimétrica

Infelizmente, a criptografia com chave pública (assimétrica) é computacionalmente intensiva. É necessário muito tempo para criptografar uma mensagem com apenas alguns parágrafos. No entanto, nem tudo está perdido, pois os melhores aspectos da criptografia com chave simétrica e da criptografia com chave pública podem ser combinados, a criptografia com chave pública e a criptografia com chave simétrica podem ser combinadas codificando-se a mensagem com o método de chave simétrica e criptografando-se a chave simétrica com o método de chave pública. Um exemplo tornará tudo mais claro. Considere Eduardo e Mônica mais uma vez. Eduardo ainda quer enviar uma mensagem à Mônica, mas dessa vez ele utilizará uma combinação de criptografia com chave pública e de criptografia com chave simétrica. Isso funciona da seguinte forma:

- **1º)** Eduardo escreve a mensagem e a codifica utilizando a criptografia com chave simétrica, com uma chave que ele cria aleatoriamente apenas

para essa mensagem. Isso é conhecido como chave de mensagem ou chave de sessão.

- **2º)** Eduardo criptografa essa chave de sessão com a chave pública de Mônica.
- **3º)** Eduardo envia a mensagem criptografada e a chave de sessão criptografada a Mônica.
- **4º)** Mônica decriptografa a chave de sessão utilizando sua chave privada.
- **5º)** Em seguida, Mônica decriptografa a mensagem usando a chave de sessão que acabou de receber.
- **6º)** Mônica agora pode ler a mensagem.
- Esse método se beneficia da força dos dois tipos de criptossistema:

A **velocidade** da criptografia simétrica e a **facilidade** dos mecanismos de distribuição de chave do sistema de criptografia com chave pública. Resolve o problema de garantir a **confidencialidade** de uma mensagem, mas não resolve o da **integridade** e da **não-repudiação**. Poderíamos simplesmente criptografar a mensagem utilizando a chave privada do emissor, como fizemos antes. Infelizmente, encontramos os mesmos problemas de desempenho discutidos anteriormente com relação a confidencialidade. Para resolver o problema, precisamos introduzir outra ferramenta útil conhecida como **message digest** (ou **hash**).

4.2.6 - Message digest ou hash

Message digest é uma função que aceita uma mensagem como entrada e produz um código de tamanho fixo como saída. Por exemplo, se tivéssemos uma função de message digest de 10 bytes, qualquer texto que executássemos através da função produziria 10 bytes de saída, como DSE32JKLnm. Cada mensagem deverá produzir facilmente um message digest aleatório. Ou seja, qualquer par de mensagens que escolhermos deverá produzir um message digest específico. Existem muitos algoritmos de message digest ou de hash, mas para que eles sejam úteis a esse propósito (considerados criptograficamente seguros), o algoritmo deverá exibir determinadas propriedades, como as seguintes:

- Sem retorno. Deverá ser difícil ou impossível determinar a mensagem que produziu uma determinada saída. Isso impedirá que alguém substitua uma mensagem por outra que tenha o mesmo message digest.
- Aleatoriedade. A mensagem deverá parecer aleatória, mais uma vez para impedir que alguém determine a mensagem original.
- Exclusividade. O message digest deverá ser exclusivo, de modo que a existência de duas mensagens com o mesmo message digest seja impossível.
- Vários message digest exibem essas propriedades. Os mais utilizados são o MD4 e os MD5, criados por Ron Rivest, da RSA Data Security Incorporated, e o SHA (Secure Hash Algorithm), criado pelo NIST (U.S. National Institute of Standards and Tecnology).

Ilustraremos como os message digest podem ser usados para oferecer não-repudiação e integridade em outro exemplo. Eduardo, mais uma vez, deseja enviar uma mensagem assinada a seus contatos, só que agora de uma forma mais eficiente. O processo funciona da seguinte forma:

- **1º)** Eduardo escreve a mensagem e cria um message digest da mensagem.
- **2º)** Eduardo criptografa o message digest com sua chave privada (ele assina a mensagem).
- **3º)** Ele envia a mensagem e o message digest criptografado a seus contatos (ele envia a assinatura).
- **4º)** Os contatos de Eduardo calculam um novo message digest da mensagem que acabaram de receber.
- **5º)** Em seguida, eles decriptografam o message digest que Eduardo lhes enviou. Para isso, utilizam a chave pública de Eduardo.
- **6º)** Por fim, eles comparam o message digest que criaram com o que Eduardo enviou (eles verificam a assinatura).

Se os dois message digests forem iguais, isso significa que somente Eduardo poderá ter enviado a mensagem. Além disso, a mensagem não poderia ter sido modificada, pois nesse caso os contatos teriam calculado um message digest que não corresponderia ao enviado por Eduardo.

4.2.7 - Message digest e criptografia de chave pública

Finalmente, combinando criptografia com chave pública e massage digests, você poderá oferecer **confidencialidade, integridade e não-repudiação**. Para ilustrar, considere que Eduardo deseja enviar uma mensagem secreta assinada para Mônica. O processo funciona da seguinte maneira:

- **1º)** Eduardo escreve a mensagem e cria um message digest da mensagem.
- **2º)** Eduardo criptografa o message digest com sua chave privada (ele assina a mensagem).
- **3º)** Ao mesmo tempo, Eduardo codifica a mensagem com base na técnica de criptografia com chave simétrica utilizando uma chave de sessão aleatoriamente escolhida.
- **4º)** Eduardo criptografa a chave de sessão com a chave pública de Mônica.
- **5º)** Agora, ele envia à Mônica a mensagem criptografada, o message digest criptografado e a chave de sessão criptografada.
- **6º)** Mônica recebe todos os três itens. Primeiro, ela decriptografa a chave de sessão usando sua chave privada.
- **7º)** Usando a chave de sessão decriptografada, Mônica decriptografa a própria mensagem.
- **8º)** Em seguida, ela calcula seu próprio message digest da mensagem.
- **9º)** Em seguida, ela decriptografa o message digest enviado por Eduardo. Para isso, Mônica utiliza a chave pública de Eduardo.
- **10º)** Por fim, ela compara os dois message digests. Se eles forem iguais, isso significa que a mensagem não foi alterada e realmente foi enviada por Eduardo.

4.2.8 - Certificados

Entende-se que, a criptografia com chave pública pode ser usada para proporcionar confidencialidade, integridade e não-repudiação. A assinatura digital exige que o verificador esteja certo de que tem uma chave pública pertencente à pessoa que assinou a mensagem. A confiança do verificador na assinatura deverá ser igual à sua confiança no proprietário da chave pública. Por exemplo, se um violador quiser forjar

documentos eletrônicos, uma estratégia seria criar um par de chaves pública/chave privada e divulgar a chave pública com o nome de outra pessoa. Quaisquer documentos assinados com a chave privada do violador serão verificados com a chave pública correspondente, uma chave pública que tenha sido anunciada como pertencente à outra pessoa!

Existem diversas estratégias para solucionar esse problema. Uma delas é trocar chaves públicas através de um meio direto, como uma reunião ou uma ligação telefônica. Infelizmente, esse método não funciona bem quando há muitas pessoas envolvidas. Uma opção melhor seria a utilização de certificados e de autoridades de certificação. Um certificado é um documento digital contento informações de identificação e uma chave pública. Em geral, os certificados têm um formato comum, normalmente baseados no padrão ITU-T X.509. Mas ainda não podemos ter certeza de que o certificado é genuíno e não é falso. Uma forma de descobrir isso é utilizar autoridades de certificação ou CAs.

Uma autoridade de certificação assina certificados de chave pública digitalmente. Ao assinar um certificado, a CA garante sua validade. No entanto um problema ainda persiste: como a chave pública da CA é distribuída? Também existem muitas estratégias para esse problema. Em uma delas, se a CA for muito conhecida, como é o caso do serviço postal americano, ela poderá divulgar amplamente sua chave pública. Outro método seria que a CA tivesse seu próprio certificado assinado por outra CA, também conhecido pelo destinatário. Essa idéia de encadeamento de certificação pode avançar ainda mais, com várias CAs organizadas em uma hierarquia onde cada CA subordinada valida sua assinatura com a assinatura de uma CA mais alta na hierarquia. Obviamente, as CAs de nível mais alto deverão reverter para o método de divulgação direta.

Quem oferecerá esses serviços? Boa pergunta. Há muito para se discutir a respeito de quem deverá manter CAs na Internet. Muitas organizações, incluindo instituições financeiras, fornecedores de aplicações e até mesmo o serviço postal americano expressaram interesse em oferecer serviços de certificação. Em 1995, com a ajuda de muitos parceiros, a RSA Data Security criou uma empresa, a Verisign, inteiramente dedicada ao fornecimento de serviços de certificação para usuários de chaves públicas, em um futuro próximo, provavelmente existirão muitas CAs na

Internet, cada uma com exigências variáveis para comprovar identidade. Algumas podem exigir que venha pessoalmente com uma cópia da sua certidão de nascimento, enquanto outras podem assinar certificados com a garantia de sua palavra. A questão aqui é que o fato de um documento ter sido assinado por uma CA não o torna necessariamente válido.

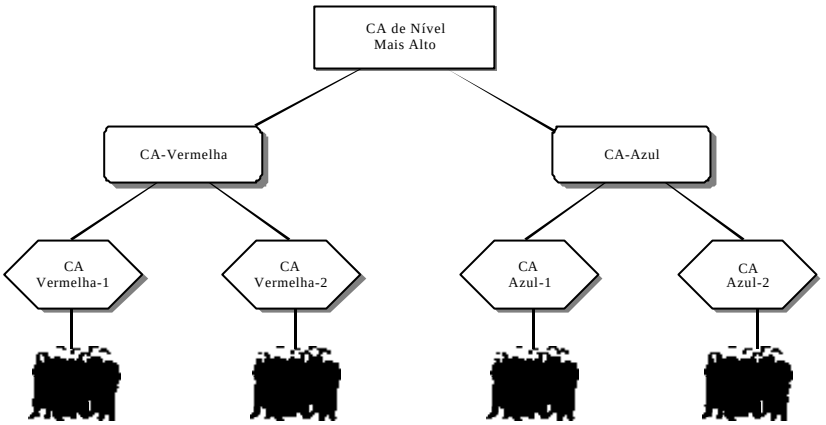

Figura 3 – *Hierarquia de CAs.*

4.2.9 - Questões práticas

Não se deve pensar que a criptografia é a solução para todas as nossas necessidades de segurança comerciais. Deve-se considerar algumas das questões de gerenciamento relacionadas à utilização da criptografia:

Tamanho da Chave. A criptoanálise, a ciência da decodificação de cifras, se baseia no fatoramento de números grandes. Conseqüentemente, quanto maior a chave, mais difícil decifrá-la. No entanto, como afirmamos anteriormente, as empresas que conduzem negócios nos Estados Unidos e no exterior são limitadas pelas leis americanas à utilização de chave de 40 bits em suas aplicações. Quarenta bits já são o bastante? Depende do que está sendo criptografado; as chaves RC4 de 40 bits podem ser decifradas com uma certa facilidade. Portanto, não é conveniente usá-las para criptografar informações durante um período muito longo. Apesar de exigir um esforço considerável, a decifração de uma mensagem criptografada com uma chave RC4 de 40 bits é possível. As chaves de 40 bits podem ser seguras para criptografar ordens de compra ou mensagens de correio eletrônico (que só precisam permanecer secretas até

que o destinatário as receba), mas talvez não sejam suficientes para proteger segredos vitais para as empresas.

Revogação de Certificado**.** O que acontece quando uma chave privada é comprometida, ou quando uma chave pública passa a ser inválida? Nesse caso, os certificados deixam de ser confiáveis, pois as informações que eles estão certificando não são mais verdadeiras. Como podemos impedir que os certificados sejam usados? Muitas autoridades de certificação divulgam periodicamente lista de certificados que não podem mais ser considerados válidos, as CRLs (certificate revocation lists). Os certificados dessas listas podem ter expirado, ou o par de chaves associadas ao certificado pode ter sido decifrado. As CRLs são muito eficientes para verificar a precisão de um certificado em um determinado momento. No entanto, as CRLs não dão qualquer garantia de que um certificado não foi revogado desde sua divulgação. Por essa razão, muitas organizações estão procurando outras soluções para lidar com a verificação de certificados.

Estrutura de CA. Já falamos sobre CAs e como elas podem ser "encadeadas" em hierarquias de certificação. Portanto, as grandes organizações podem optar por ter dentro delas várias CAs (uma para o departamento de pesquisa, outra para o departamento de marketing e assim por diante) e ter uma única CA de nível mais alto para certificar as CAs dos departamentos. No entanto, ter uma única CA na empresa cria um "único ponto de falha", pois o comprometimento do par de chaves da CA corporativa pode resultar na perda das chaves de todos os funcionários da empresa. Outras empresas optam por uma estrutura plana de CAs, na qual cada CA departamental tem muitas outras CAs parceiras, que correspondem aos outros departamentos da empresa. É melhor ter uma hierarquia de CAs, na qual o comprometimento de uma única CA pode resultar no comprometimento de todos os certificados da empresa, ou é melhor ter uma estrutura plana, na qual várias CAs devem ser controladas e devem trocar mensagens umas com as outras, fazer ou não fazer caução. Esse é um dos assuntos mais debatidos no que se refere à criptografia. Muitas empresas afirmam que, como a comunicação dos funcionários é propriedade da empresa, a organização deverá ter acesso às chaves dos funcionários, recuperar mensagens (quando houver desligamento de funcionários ou quando eles perderem suas chaves, por exemplo). Por outro lado, a maior parte dos defensores da privacidade é veementemente contra essa

idéia, citando a emenda federal (lá nos E.U.A) que garante os direitos dos funcionários à privacidade.

O Que Fazer com Todas Essas Informações? O arquivamento de chaves e de dados criptografados (mensagens de correio eletrônico criptografadas, ordens de compra assinadas e assim por diante) é uma questão extremamente difícil. Muitas empresas têm de armazenar informações durante muito tempo, devido a regulamentos ou a outras restrições. Mas, com freqüência, armazenar mensagens ou ordens de compra pode envolver muito mais do que a simples manutenção de informações. Considere, por exemplo, o armazenamento de ordens de compras assinadas. Como as assinaturas só podem ser verificadas com a chave pública apropriada, todas as chaves públicas (e suas cadeias de certificação) devem ser guardadas para sempre. Mais uma vez, para grandes empresas, isso pode ser complicado, o que estamos tentando mostrar é que, assim como outras soluções técnicas, algumas decisões importantes em termos de gerenciamento devem ser tomadas antes da implementação da criptografia. Se uma empresa considerar essas questões antecipadamente, a utilização da criptografia será mais fácil.

4.3 - AUTENTICAÇÃO

4.3.1 - Autenticação de Usuário

Os serviços de autenticação são um elemento importante em qualquer sistema de segurança na Internet. As entidades que se comunicam na Internet devem ter alguma forma de verificar com quem estão “falando”. Essas entidades podem ser pessoas que estejam operando sistemas de computador, ou talvez dois computadores que estejam se comunicando através de um processo automático. A exemplo do que acontece no mundo “real”, são necessários diferentes graus de autenticação. Diversos métodos e aplicações oferecem serviços de autenticação com diferentes graus de certeza. Em geral, quanto maior for à certeza necessária para identificar um usuário na Internet, mais alto será o custo e mais difícil será a utilização do método. No lugar de senhas reutilizáveis, quatro técnicas principais são utilizadas para autenticação. Essas técnicas se baseiam na localização de uma pessoa ou computador, ou no que essa pessoa ou computador conhece, tem ou é. Ao lidar com pessoas, você deverá usar mais de uma dessas técnicas para autenticar a identidade delas.

4.3.2 - Autenticação baseada na localização

A autenticação baseada na localização é muito utilizada. Em geral, ela é implementada através de sistemas de “callback” ou de ID de chamada. Essa técnica, sozinha, é boa, mas não é à prova de falha: um invasor poderia penetrar em um local seguro ou até mesmo enganar os computadores da companhia telefônica ou desviando o callback para outro lugar. Muitos sistemas de rede se baseiam em um identificador de usuário e no endereço de rede do sistema original para fazer a autenticação. Ou seja, o autenticador assume que a identidade da origem pode ser inferida com base no endereço (de rede) de onde os pacotes foram enviados. Por exemplo, um servidor deverá confiar inteiramente no usuário Eduardo do sistema sem qualquer mecanismo de autenticação adicional. A autenticação se baseia unicamente no fato de que a comunicação com um ID de usuário tem origem em um determinado host com um endereço IP específico. A autenticação baseada em endereço é segura contra ataques de ingerência e adivinhação porque todos os aspectos da autenticação já são conhecidos. Mas ela está sujeita a muitas outras ameaças, incluindo:

Invasão de Sistemas Confiáveis. Sistemas considerados como confiáveis com base em seu endereço de rede podem ser invadidos por um intruso. Uma vez que tenha invadido o sistema confiável, o intruso poderá facilmente se fazer passar por outro usuário e conseguir a autenticação, falsificação de Endereço. Esse tipo de ataque, no qual o invasor configura um computador para fazê-lo passar por um sistema confiável está se tornando cada vez mais comum. Uma forma desse ataque, conhecida como spoofing do IP, foi explicada no item 12.4.

4.3.3 - Autenticação baseada no que o computador “conhece”

A autenticação baseada naquilo que alguém conhece talvez seja a técnica mais antiga e mais comum. Em geral, esse método é implementado através da utilização de uma combinação de identificador e senha do usuário. O problema é que não há uma forma infalível de garantir que apenas pessoas confiáveis conheçam a senha adequada, de fato, inúmeros problemas são associados à utilização de senhas. As formas de violação de senhas são inúmeras.

As senhas ocasionais representam uma nova variante dos tradicionais esquemas de senha. Para acessar um host, o usuário tem de informar um identificador e uma senha, exatamente como acontece em um sistema de senha comum; no entanto, a senha é válida apenas uma vez. Ou seja, o usuário informa uma senha específica a cada vez que precisa se autenticar para o sistema. Nesse sistema, uma lista de senhas é computada antecipadamente, e os resultados são impressos para facilitar a entrada. Um exemplo desse tipo de sistema é o S/key desenvolvido na Bellcore**.**

4.3.4 - Autenticação baseada no que o computador “é”

Uma forma menos utilizada de autenticação se baseia naquilo que uma entidade é ou representa. Essa categoria abrange os atributos físicos (como as impressões digitais) de pessoas ou computadores. Se utilizada corretamente, essa forma de autenticação pode ser muito interessante. Por exemplo, um sistema que fosse capaz de interpretar impressões digitais seria praticamente à prova de falha, além de ser fácil de usar. Infelizmente, esses tipos de sistemas biométricos são muito caros e ainda estão em fase de experiência, poucos sistemas no mercado fazem autenticação verificando os atributos do computador. Por exemplo, o sistema de autenticação pode registrar o tipo da CPU, o tamanho do disco rígido, as aplicações instaladas e outros itens para criar uma “impressão digital” do computador. Quando um usuário estabelece login, o sistema verifica sua “impressão digital” antes de permitir o acesso.

4.3.5 - Autenticação baseada no que o computador “tem”

A última forma de autenticação comumente usada se baseia naquilo que uma pessoa ou entidade possui. Por exemplo, o fato de alguém ter uma placa de computador especial pode ser usado para verificar sua identidade. Diversos dispositivos são comumente usados para esse objetivo, como smart cards.

Em geral, esses dispositivos são protegidos por senhas. Após sucessivas adivinhações erradas, o dispositivo deixa de funcionar. Todos esses dispositivos são mais difíceis de espionar ou duplicar do que os cartões de crédito tradicionais.

4.3.6 - A seleção de uma estratégia de autenticação

A aplicação e a natureza dos dados que estão sendo protegidos impõem o tipo de autenticação utilizado. Em geral, quanto mais tipos de autenticação forem utilizados (baseados na sua localização, no que você conhece e no que você tem), mais segura será a transação. Com a utilização de apenas uma técnica, como senhas ou callback, a configuração é mais fácil e o custo é mais baixo, mas há grandes possibilidades de um intruso anular essa técnica. Utilizar mais de uma técnica (autenticação por dois fatores), como uma senha e um dispositivo portátil, aumenta drasticamente a segurança do sistema. As principais desvantagens do sistema de dois fatores são o custo mais alto e a dificuldade de administração, para qualquer tipo de uso mais sério da Internet, são necessárias técnicas de autenticação por dois fatores mais rígidas que utilizem a criptografia. A Internet já foi lugar relativamente confiável, e podiam-se utilizar esquemas de autenticação mais simples, como as senhas. Apesar de isso não ser mais verdadeiro nos dias de hoje, a confiança nas senhas persiste.

4.4 - FIREWALL

4.4.1 - Visão geral

Um firewall é usado para regular o tráfego entre duas redes. Pode-se dizer que é uma barreira “inteligente” entre essas redes, através da qual só passa tráfego autorizado. Esse tráfego é examinado pelo firewall em tempo real e a seleção feita de acordo com a regra “o que não foi expressamente permitido, é proibido”**.** Para criar as regras através das quais o firewall selecionará o tráfego, é preciso saber os serviços, os endereços e as estações para as quais o tráfego será permitido ou negado. A orientação do *firewall* quanto à passagem de recursos pode ser resumida a duas posições diametralmente opostas:

Tudo o que não for especificamente permitido é proibido - posição que determina que o firewall deve bloquear todo e qualquer tráfego e que cada serviço ou aplicação desejada deve ser implementada caso-a-caso. Esta abordagem é, sem dúvida, a mais segura e recomendada. Sua desvantagem é dar à questão da segurança maior peso que à questão da facilidade de uso, tudo o que não for especificamente proibido é permitido - posição que determina que o firewall deve permitir a passagem de todo e qualquer

tráfego, e que serviços ou aplicações potencialmente perigosas devem ser desabilitadas caso-a-caso. Esta abordagem cria um ambiente mais flexível, oferecendo mais serviços aos usuários, mas sua desvantagem é colocar a facilidade de uso num patamar de importância maior que a segurança. Tradicionalmente, essas duas redes têm sido a Internet e a rede corporativa, mas os firewalls também podem ser usados entre duas redes quaisquer com diferentes necessidades de segurança. Os firewalls podem ser utilizados praticamente em qualquer ponto da rede, e são cada vez mais usados entre duas redes internas, sobre as quais uma organização exerce diferentes níveis de controle e tem diferentes exigências de segurança (tais como o ambiente de pesquisas, no qual deve haver um alto nível de conectividade e poucas restrições, e a LAN do departamento de recursos humanos e folha de pagamento, onde deve haver um grande número de restrições). Este trabalho pressupõe que as duas redes envolvidas são a rede corporativa e a Internet. Assim, vamos nos referir às duas redes como “interna”, ou a rede na qual estão as propriedades a serem protegidas, e “externa”, que corresponde à Internet, a melhor maneira de se entender como trabalha um firewall é imaginá-lo como sendo um guarda, ou sentinela, da rede, que inspeciona a documentação para os pacotes que chegam e depois decide se dará passagem ou não**.**

Além disso, os firewalls também servem para “ocultar” algumas máquinas de outras. Além de regular o tráfego que chega e que sai das máquinas, alguns firewalls podem ser configurados para mascarar a topologia interna de uma rede através da restrição das divulgações do DNS (Domain Name System) e dos endereços de rede no tráfego de saída, talvez uma das maiores vantagens do firewall é que ele oferece um único ponto de controle para a segurança da rede pelo qual todo o tráfego deve passar antes de entrar na rede da corporação ou sair dela. Os firewalls também oferecem um único ponto de administração da segurança sendo um ótimo ponto para auditoria e Monitoração. Assim os firewalls tendem a ser os principais alvos para ataques externos o que nos impõe como prioridade garantir a segurança da máquina. Por outro lado, os firewalls apresentam um único ponto para uma falha na segurança. Se o firewall for comprometido, o perímetro seguro será violado e um intruso terá acesso livre a toda a rede da corporação. Por essa razão, os melhores firewall são compostos de vários “blocos”, cada um dos quais oferece algum reforço e aumenta a segurança do sistema firewall.

4.4.2 - O que os firewalls não podem fazer

Os firewalls não são panacéia para todos os males de segurança na Internet. Há muitas tarefas que os firewalls não são capazes de executar:

Não garantem proteção contra ameaças internas. Um firewall pode proteger de quase todos os ataques externos baseados na Internet, mas nada faz contra ataques internos. A ameaça interna é muito importante e não deve ser ignorada. Para tratar dela, muitas companhias preferem implantar firewalls internos entre as sub-redes. Os firewalls garantem indiretamente alguma integridade aos dados da rede interna, ao protegê-los de acessos não autorizado, mas com relação a vírus a questão não é tão simples. Algumas empresas tentam utilizar firewalls também para detectar vírus, no entanto, a verificação de todo o tráfego recebido não é viável, e a queda do desempenho da rede causada pela inspeção de cada pacote se torna insuportável. Além disso, é impossível verificar todos os formatos de arquivos binários na tentativa de localizar milhares de vírus conhecidos. A única maneira real de verificar a presença de vírus no tráfego recebido é restringir os locais para onde os arquivos binários serão trazidos, fazer a verificação off-line e depois entregá-los ao usuário.

Não garantem a autenticidade da origem dos dados. Por sua própria natureza, um firewall só pode ver um “instantâneo” do pacote; o firewall não tem qualquer controle sobre como o pacote foi criado, ou que ele faz quando chega a seu destino. Um grande problema de segurança com o TCP/IP é que qualquer um pode gerar uma mensagem se fazendo passar por outra máquina (ataques de “spoofing”). Não garantem proteção para tráfego alternativo. Um firewall não pode oferecer proteção contra um tráfego que não passa por ele. Um “perímetro de rede seguro” implica que todos os pontos de entrada da rede sejam seguros, e não apenas a entrada principal. Pouco adianta um firewall grande e de alto custo, se a empresa tem modems de discagem direta nas mesas dos funcionários.

4.4.3 - Técnicas de firewalls

Podemos dividir em três tipos os firewalls utilizados pelas empresas:

- Filtros de pacotes baseados no roteador e no host;
- Filtros “inteligentes” baseados no host;
- Servidor Proxy e gateways de aplicações baseados no host.

Algumas soluções de firewalls mais “robustas” fazem uso de uma combinação das técnicas mencionadas.

- Filtros de pacotes. Talvez a maneira mais fácil (e de custo mais baixo) de implementar um firewall seja no roteador que conecta a rede privada à Internet. Podemos usar a capacidade de filtragem do roteador para implementar segurança. De fato, até alguns anos atrás, era assim que os firewalls eram implementados. Esses roteadores utilizam o conceito de filtragem de pacotes para controlar tipo de tráfego que passa por ele. Firewalls que operam no nível da rede geralmente baseiam suas decisões nos endereços de origem e destino e nas portas contidas em pacotes IP individuais. Um roteador simples é a forma mais típica de um firewall operando no nível da rede. Um roteador não é capaz de decisões sofisticadas sobre o conteúdo ou a origem de um pacote. No outro extremo, firewalls que atuam no nível da aplicação, são geralmente computadores executando servidores proxy, que não permitem fisicamente a existência de tráfego entre redes, e que efetuam elaboradas operações de verificação nos dados que por eles trafegam. Além disso, firewalls deste tipo são excelentes também como tradutores de endereços de rede (NAT), já que o tráfego "entra" por um lado e "sai" por outro, depois de passar por uma aplicação que efetivamente mascara a origem da conexão inicial. Este tipo de firewall é certamente menos transparente para os usuários e pode até causar alguma degradação no desempenho. Apesar de originalmente terem sido projetados para controlar a largura de banda em ligações muito utilizadas, os filtros de pacotes baseados no roteador oferecem uma razoável funcionalidade em termos de segurança e, com o tempo, foram reconhecidos como uma importante ferramenta para a segurança. Até hoje uma grande razão para sua popularidade é a incrível transparência com que os filtros baseados no roteador funcionam. A maioria dos filtros pode ser implantada sem a menor inconveniência para o usuário final, que às vezes nem fica sabendo de sua existência. Entretanto, a filtragem dos pacotes não se limita aos roteadores. Diversos filtros baseados no host estão disponíveis em domínio público. Assim como os roteadores que os antecederam, esses hosts utilizam as técnicas de filtragem de pacotes descritas a seguir para implementar o controle de tráfego no ponto regulador de uma rede.

O princípio básico por trás dos filtros de pacotes é simples. Com base na tecnologia “store-and-forward” (armazenamento e encaminhamento) dos roteadores, um

roteador ou host receberá um pacote em uma interface, comparará as informações em seu cabeçalho com um conjunto de filtros e então decidirá se deixa o pacote passar, se o abandona inteiramente ou se o "rejeita" (enviando uma mensagem ICMP de volta a ponto de origem indicando que o pacote foi abandonado). Apesar de os parâmetros específicos nos quais um filtro de pacotes baseia suas decisões variarem de um produto para outro, a maioria dos filtros de pacotes leva em consideração os seguintes critérios**:**

- A direção do tráfego (da interface para a rede interna ou da rede para a interface);
- A interface na qual o tráfego foi recebido ou para a qual se destina;
- O tipo de protocolo (por exemplo, IP, ICMP, TCP, UDP, IPX);
- Os endereços IP de origem e de destino;
- A porta TCP ou UDP de origem e de destino;
- A informação sobre o "estado" do TCP.

A maioria dos fornecedores de roteadores já incorpora os filtros de pacotes no software do roteador. Esses filtros são, com freqüência, usados como listas de acesso nas interfaces dos roteadores e segue, com algumas variações, o seguinte modelo de sintaxe:

<lista de acesso #> <permit/deny> <protocolo> <origem> <destino> <opções>

Embora haja variação de sintaxe entre diferentes fornecedores o que pode trazer dificuldades para decifrarmos as listas de acesso de cada um deles, a sintaxe do filtro identifica o tráfego por sua origem e seu destino. Além disso, podemos identificar a "porta" de destino do tráfego. Alguns filtros também permitem que o tráfego seja identificado com base em sua "porta" de origem, mas muitos sistemas não aceitam esse recurso. Como exemplo, consideremos uma empresa que deseja bloquear todo o tráfego que chega à sua rede usando o protocolo telnet, que tem a porta 23 como destino. Nossa lista de acesso seria assim:

- **LISTA AÇÃO Prot. ORIGEM ESTINO**
- **Access-list 1 deny tcp all inside port 23**

Essa lista informa ao roteador para "recusar" todos os pacotes TCP, sem levar em conta sua origem, que tenham como destino qualquer host da rede interna que utilize a porta de destino 23 (a porta do telnet). Os filtros de pacotes, entretanto, têm algumas limitações inerentes. Imaginemos uma organização que deseja controlar acesso proveniente da Internet, mas quer que seus funcionários utilizem a Internet à vontade.

Essa empresa pode, com facilidade, bloquear o tráfego destinado aos servidores internos telnet, de correio ou da Web usando uma regra de lista de acesso. Entretanto, se a empresa fosse bloquear todo o tráfego recebido em todas as portas das máquinas internas, o tráfego de retorno para as solicitações emitidas (tais como as respostas a uma solicitação de download de páginas da Web) estaria bloqueado junto com as tentativas de conexão não-autorizadas. Por outro lado, se abrir todas as portas não-privilegiadas, a empresa permite não só que os servidores externos respondam a pesquisas de clientes, mas também que clientes externos estabeleçam conexões com servidores internos que por acaso estejam sendo executadas em portas de numeração alta, maiores detalhes sobre esses ataques e “portas” podem ser encontrados nas RFC’s da Internet.

Além de suas limitações técnicas, os filtros de pacotes, em especial os baseados em roteadores, têm limitações significativas. Uma delas é a incapacidade de alguns roteadores de manter um log do tráfego. A maioria das organizações gosta de monitorar o tráfego que atravessa o firewall e os pacotes que são abandonados pelo filtro de pacotes. Sem um tipo qualquer de log de pacote, é muito difícil assegurar a integridade de um firewall e determinar os padrões de uso da Internet para reavaliar decisões políticas em relação a protocolos específicos. Recentemente, diversos fornecedores de roteadores começaram a apresentar recursos de log de pacotes, mas eles não têm a capacidade de fazer um “log variável”, ou seja, a habilidade de oferecer diferentes níveis de log para os diferentes tipos de tráfego.

Uma segunda limitação dos filtros de pacotes é sua incapacidade para desempenhar a autenticação do usuário. Como foi visto anteriormente qualquer forma de autenticação “rigorosa” (tais como, senhas ocasionais ou um cartão de token) é vista como um requisito fundamental para o tráfego cuja origem é a Internet. Se não tiverem os recursos necessários para proporcionar uma autenticação rigorosa, as organizações que utilizam filtros de pacotes baseados no roteador terão de prover essa capacidade através de um mecanismo alternativo, o principal inibidor ao uso de filtros de pacotes baseados no roteador, entretanto, é a falta de ferramentas de administração. Para entendermos como funciona a filtragem de pacotes, precisamos atentar para a diferença entre um roteador comum e um screening router. Um roteador comum simplesmente observa o endereço de destino de cada pacote e decide qual o melhor caminho para enviar o pacote ao seu destino. Então, a decisão de como tratar o pacote é baseada

somente no endereço de destino. Existem, então, duas possibilidades: ou o roteador sabe como enviar o pacote ao seu destino, e o faz, ou não sabe, e retorna-o à origem, com uma mensagem ICMP de "destino inalcançável". Um screening router, por outro lado, observa as características do pacote mais detidamente. Além de determinar se pode ou não rotear o pacote ao seu destino, também determina se deve fazê-lo, de acordo com as regras de segurança que o roteador deve fazer cumprir. Na figura 3 abaixo, observamos a posição típica de um screening router num sistema.

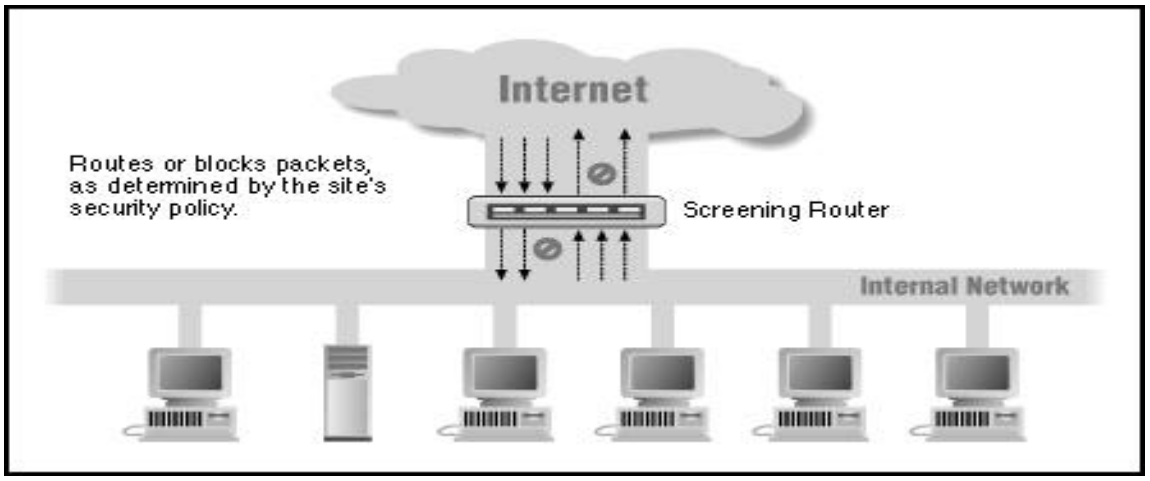

Figura 3 - *Usando um screening router para a filtragem de pacotes.*

A maioria dos sistemas firewall existentes em conexões à Internet baseiam-se em um screening router, uma decisão motivada principalmente pelo baixo custo desta solução, já que a filtragem de pacotes é uma característica incluída como parte integrante dos softwares que acompanham qualquer roteador. Além disso, mesmo que o screening router não seja a única ferramenta de proteção, certamente estará presente mesmo em arquiteturas mais elaboradas, no geral, os filtros de pacotes baseados no roteador representam um pesadelo administrativo para as organizações e também para os administradores de firewalls.

- Filtros “inteligentes”. Recentemente, diversos fornecedores de firewalls começaram a tratar das falhas dos filtros de pacotes padrão. Eles projetaram um novo tipo de filtro de pacotes que chamamos de “filtro inteligente”. Os filtros inteligentes são filtros baseados em hosts que desempenham as mesmas funções gerais que os filtros de pacotes padrão, mas que têm maior funcionalidade e não apresenta parte dos problemas associados aos filtros padrão.

Para começar, a maioria dos filtros inteligentes inclui uma interface GUI administrativa para facilitar a configuração dos filtros de pacotes. Em vez de exigir o conhecimento de alguma linguagem misteriosa, essa interface recebe entradas em um formato legível e amigável, e as traduz de uma forma transparente para uma linguagem de máquina. Um filtro inteligente permite sete níveis de log, que variam de uma simples contagem dos pacotes a um mecanismo que aciona o administrador (através de pager) caso algum tipo de evento aconteça. Também resolve algumas das limitações das filtragens de pacotes encontradas em muitos roteadores, uma vantagem final dos filtros inteligentes sobre os filtros de pacotes padrão é que eles aceitam autenticação. A maioria dos filtros inteligentes se baseia no host e aceita alguma forma de autenticação para serviços interativos, tais como telnet e FTP.

- Servidores proxy e gateways**.** Nos firewalls de filtragem, descritos anteriormente, todo o tráfego passa pelo firewall sem que a origem e o destino tenham conhecimento da existência do roteador entre eles. As máquinas internas são visíveis para a rede externa. Os servidores proxy implementam uma outra visão dessa situação. Em vez de adotar a abordagem transparente dos roteadores e de outros filtros de pacotes, os servidores proxy adotam uma abordagem “store-and-forward”, na qual encerram a conexão de chegada a partir da origem e iniciam uma segunda conexão para o destino. Em geral, os servidores proxy têm várias interfaces de rede, o que permite que eles se comuniquem com várias redes. Por essa razão, as máquinas nas quais o servidor proxy é configurado são quase sempre chamadas de “gateways de base dupla”. Um gateway de base dupla pertence a duas redes e funciona como ponto regulador entre elas. Para estabelecer uma conexão entre as duas redes, o usuário teria que primeiro fazer um login com o gateway para depois estabelecer conexão com o destino desejado. Se o usuário estiver tentando recuperar alguma informação desse destino (digamos através de FTP), o usuário terá primeiro que depositar a informação no gateway e depois recuperá-la do gateway para sua máquina individual, essa abordagem tem um grande número de problemas. A maioria dos usuários não tem paciência para fazer vários logins em várias máquinas, nem quer memorizar mais de uma senha para a máquina do gateway, para não falarmos de outros inconvenientes, que contribuirão para a vulnerabilidade da rede. Os servidores proxy enriquecem muito o gateway de base dupla. Apesar de o conceito geral de store-and-forward ainda fazer sentido, o servidor proxy facilita a vida do

usuário, pois estabelece a segunda conexão com a máquina remota para o usuário (daí o nome proxy, que em inglês significa procuração). Os servidores proxy também evitam a necessidade de o usuário acessar o sistema operacional no firewall.

O usuário ainda estabelece uma conexão com o gateway, mas em vez de realizar o login no próprio gateway, o usuário pode escolher, a partir de um menu que lhe é apresentado, e determinar aonde deseja ir. O gateway consulta, estão, uma lista de conexões permitidas e, a partir dela, nega o acesso ou estabelece a conexão com o destino. A partir daí, a conexão prossegue com um certo nível de transparência (o usuário pode observar a conexão com o servidor de destino). Os servidores proxy oferecem inúmeras vantagens sobre os gateways de base dupla genéricos. Para começar, ao contrário dos gateways de base dupla, eles não exigem que o usuário tenha acesso ao sistema operacional. As vantagens, nesse caso, devem ser óbvias: quanto menos for possível acessar o sistema operacional, menores as chances de uma invasão. Além disso, os servidores proxy não exigem que os usuários façam várias conexões através de diferentes máquinas. Os servidores proxy dão ao usuário a impressão de que a conexão é completamente transparente após ser estabelecida; não há necessidade de uma transferência de dados manual do servidor para o gateway, e do gateway para a máquina local, a principal vantagem dos servidores proxy, porém, é que, ao contrário dos roteadores e filtros de pacotes, eles “escondem” o host interno do servidor de destino. Para empresas que não desejam que sua rede interna seja visível ao mundo exterior, essa é uma grande vantagem.

4.4.4 - Tipos de servidores proxy

Em geral, existem três tipos de servidores proxy: servidores proxy de aplicação específica, proxies de aplicação genérica e servidores proxy de “circuito”, sendo que cada um tem muitos recursos. **Servidores proxy** de aplicação específica**.** Como o nome sugere, os servidores proxy de aplicação específica, como os descritos para o FTP, oferecem serviços de proxy para uma única aplicação específica. Embora essa capacidade possa parecer um tanto limitado, ela possibilita algumas decisões de aplicação específica. Por exemplo, a possibilidade de restringir o upload de arquivos, ao mesmo tempo em que permite o download; ou a possibilidade de restringir a submissão de informações através de formulários de Web, enquanto permite a recuperação

ilimitada de informações da Web. Os servidores proxy de aplicação específica são a forma mais comum de servidor proxy em uso hoje em dia, e a maioria dos servidores proxy dos produtos de firewall comerciais é desse tipo. **Servidores proxy** genéricos. Os servidores proxy de aplicação específica têm uma desvantagem óbvia. Embora sejam perfeitos para serviços como telnet, FTP ou a Web, aplicações largamente utilizadas, eles não estão disponíveis para muitos outros serviços, tais como o Netnews, SMB (muito usado no Windows NT) ou aplicações específicas de cada empresa. Para essa finalidade, alguns produtos de firewall oferecem um tipo de "proxy genérico". Esse proxy é apenas um "packet relay" que aceita as conexões recebidas, consulta algum tipo de tabela de configuração para saber quais são as conexões permitidas e estabelece conexão com seu verdadeiro destino. Em sua maioria, os servidores proxy genéricos em uso atualmente fazem parte de pacotes de firewall mais completos. Esses pacotes incluem um proxy genérico para as aplicações que não são aceitas pelos servidores proxy de aplicação específica, apesar de serem extremamente úteis em um ambiente onde haja uma relação de "muitos para uns", eles não são eficientes em uma situação de "um para muitos" ou de "muitos para muitos", quando os usuários talvez precisem acessar vários servidores**.**

Proxies de circuito. Um terceiro tipo de servidor proxy baseia-se livremente no conceito de proxy genérico. Em vez de agir somente como um "packet", porém, esse tipo de servidor proxy permite que vários clientes se comuniquem com vários servidores e oferece uma transparência quase completa tanto para o usuário quanto para o servidor. O resultado dessa estratégia é criar um circuito virtual fim a fim entre o cliente e o destino final. Por essa razão, esse tipo de proxy é com freqüência chamado de "gateway de circuito" ou "proxy de circuito". Para oferecer esse nível de transparência, os proxies de circuito em geral exigem que a aplicação cliente tenha conhecimento da existência do servidor proxy. Por isso, a implementação de um proxy de circuito quase sempre exige a troca de cada cliente TCP/IP por outro que possa reconhecer que deve se comunicar através de um servidor proxy. Na maioria das empresas de médio a grande porte, essa exigência não faz sentida. O proxy de circuito mais comum é o SOCKS, desenvolvido por David e Michele Koblas em 1991. O SOCKs, na verdade, oferecem um proxy de circuito acompanhado de um conjunto de bibliotecas clientes que pode ser usado para desenvolver clientes que reconheçam o proxy. O SOCKs é o servidor proxy

mais genérico que você pode encontrar. De certo modo, ele não é muito diferente de um filtro inteligente, exceto pelo fato de que se baseia no modelo store-and-forward de um servidor proxy, e não no modelo transparente de um filtro de pacote.

4.4.5 - Arquiteturas de firewalls

Freqüentemente as empresas implementam seu projeto de firewall baseado em apenas uma máquina, seja ela um computador ou um roteador. Projetos mais complexos para firewalls mais rigorosos, são compostos de várias partes, o que define diferentes arquiteturas. Os cinco tipos mais comuns de arquiteturas de firewalls são**:**

- Roteador com triagem;
- Gateways de base dupla;
- Gateway host com triagem;
- Sub-rede com triagem;
- Firewall “belt and suspenders”.

Roteador com triagem. A maneira mais simples de implementar um firewall é implantar filtro de pacotes no próprio roteador. Essa arquitetura é completamente transparente para todas as partes envolvidas, mas nos deixa com um único ponto fraco. Além disso, como os roteadores são projetados para rotear o tráfego, seu modo de falha padrão é a passagem de tráfego para outra interface (apesar de a maioria dos roteadores incluir a declaração “... e rejeita todo o resto**”** no final da lista de acesso, existe a possibilidade de uma falha no mecanismo de segurança). Além disso, os roteadores com triagem tendem a violar o princípio do ponto regulador dos firewalls. Embora em algum momento todo o tráfego passe pelo roteador, ele simplesmente conduz os elementos a seu destino final. Portanto, todos os destinos em potencial dentro da rede, e não apenas um ponto regulador, deve ser seguro. Embora os roteadores com triagem possam ser elemento importante na arquitetura de um firewall, sozinhos não resolvem os problemas de segurança.

Gateways de base dupla. Nesta arquitetura uma única máquina com duas interfaces de rede é colocada entre duas redes: o gateway de base dupla. Esses gateways podem ser usados não só como gateways de base dupla genéricos, nos quais todos os usuários devem estabelecer login antes de passarem para a próxima rede, mas também como hosts para servidores proxy, que não necessitam de contas de usuários. Em

termos de recursos contra falhas, os gateways de base dupla estão um passo à frente dos roteadores com triagem. Como a maioria dos sistemas baseados no host tem, por definição, a opção de encaminhamento de pacotes desativada, é praticamente impossível controlar o tráfego sem configurar o host para essa finalidade. Portanto, em geral, o modo de falha dos gateways de base dupla é mais robusto do que o dos roteadores com triagem.

Gateways host com triagem. Os hosts e os roteadores podem ser usados em conjunto em uma arquitetura de firewall. Na arquitetura de gateway host com triagem, o roteador ainda é a primeira linha de defesa. A filtragem de pacotes e o controle de acesso são executados no roteador. O roteador só permite o tráfego explicitamente por regras específicas e restringe as conexões recebidas pelo gateway host. Esse gateway executa as seguintes funções:

- Funciona como servidor de nomes para toda a rede corporativa.
- Funciona como servidor de informações “públicas”, oferecendo ao mundo acesso através da Web e por FTP anônimo.
- Funciona como um gateway a partir do qual se estabelece a comunicação externa com máquinas internas.

Gateways host com triagem são implementações populares, pois permitem que as empresas concedam a seus usuários interno acesso total à Internet, apesar de limitarem um pouco o acesso à sua rede a partir da Internet. São relativamente fáceis de implementar, pois utilizam um roteador padrão e uma única máquina host. Os gateways hosts com triagem são bem melhores que roteadores com triagem e que os gateways de base dupla.

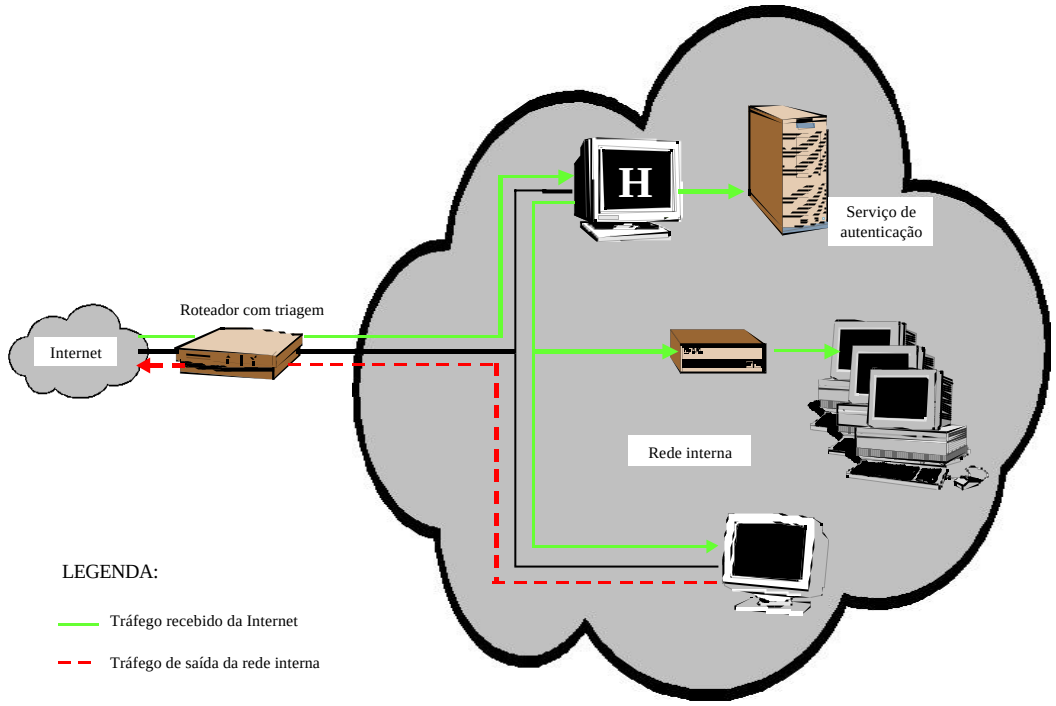

Figura 4 – G*ateway host com triagem*

Sub-rede com triagem. A arquitetura de sub-rede com triagem utiliza a idéia de um gateway host com triagem, mais vai um pouco mais além. O roteador com triagem continua presente como primeiro ponto de entrada para a rede da corporação e faz a triagem do tráfego entre a Internet e os hosts públicos. Em vez de um único gateway, como acontece na técnica de gateway host com triagem, entretanto, as funções desse gateway são distribuídas por vários hosts. Desta forma, um dos hosts poderia ser um servidor da Web, outro poderia ser um servidor de FTP anônimo e o terceiro poderia ser o host do servidor proxy, a partir do qual todas as conexões à rede interna da corporação seriam estabelecidas. Do ponto de vista funcional, a sub-rede com triagem é semelhante ao gateway host com triagem: o roteador protege o gateway contra a Internet, e o gateway protege a rede interna contra a Internet e outros hosts públicos. Uma vantagem distinta que a sub-rede tem sobre o gateway com triagem é que é muito mais fácil implementar uma sub-rede com triagem usando hosts “stripped down”; ou seja, cada host da sub-rede pode ser configurado para executar os serviços que deve oferecer; com isso, o intruso passa a ter menos alvos potenciais em cada máquina. Além disso, as máquinas da sub-rede podem se tornar acessíveis para os clientes da rede interna, bem como para os clientes baseados na Internet. As máquinas internas não precisam tratar as

máquinas da sub-rede de forma diferente da que tratam qualquer outra máquina "externa" na Internet. De fato, se essa estratégia for adotada, uma sub-rede com triagem poderá aumentar substancialmente a segurança potencial de uma rede, pois é improvável que o comprometimento de uma máquina externa (exceto, talvez, pelo gateway onde são executados os servidores proxy) permita o acesso à rede interna. Na arquitetura de sub-rede com triagem incluímos outra categoria de rede entre a externa (Internet) e a interna (rede da empresa) que alguns autores chamam de "rede de perímetro" ou rede DMZ (Demilitarized Zone).

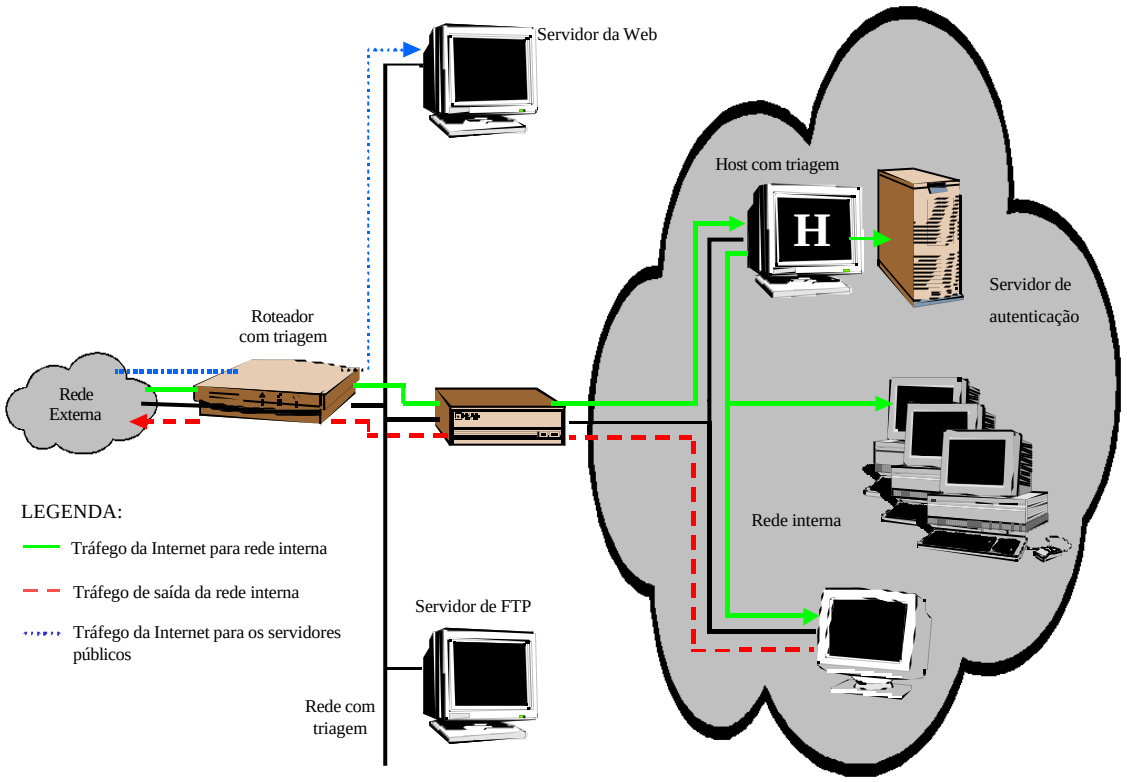

Figura 5 – *Sub-rede com triagem.*

Firewall "belt and suspenders". Esta arquitetura utiliza o conceito de sub-rede com triagem, aprimorando-o, no entanto. Os princípios são os mesmos da arquitetura de sub-rede: um roteador com triagem externo protege as máquinas "públicas" da Internet. Em vez de um gateway que executa um software de servidor proxy e ao mesmo tempo protege a rede interna, essas funções são divididas: o host do servidor proxy agora reside na sub-rede DMZ, enquanto um roteador com triagem interno serve para proteger a rede interna contra as máquinas públicas. Essa arquitetura é com freqüência chamada de arquitetura "belt and suspenders" (literalmente, "cinto e suspensórios").

A arquitetura belt and suspenders é só um pouco diferente da sub-rede com triagem, mas essa diferença é muito importante do ponto de vista da segurança. Enquanto a sub-rede com triagem conta com os servidores proxy para controlar o acesso à rede interna, a estratégia belt and suspenders utiliza o servidor proxy como a primeira linha de defesa em termos de autenticação. Além disso, o roteador interno serve de apoio para o servidor e protege a rede interna contra as máquinas da rede pública.

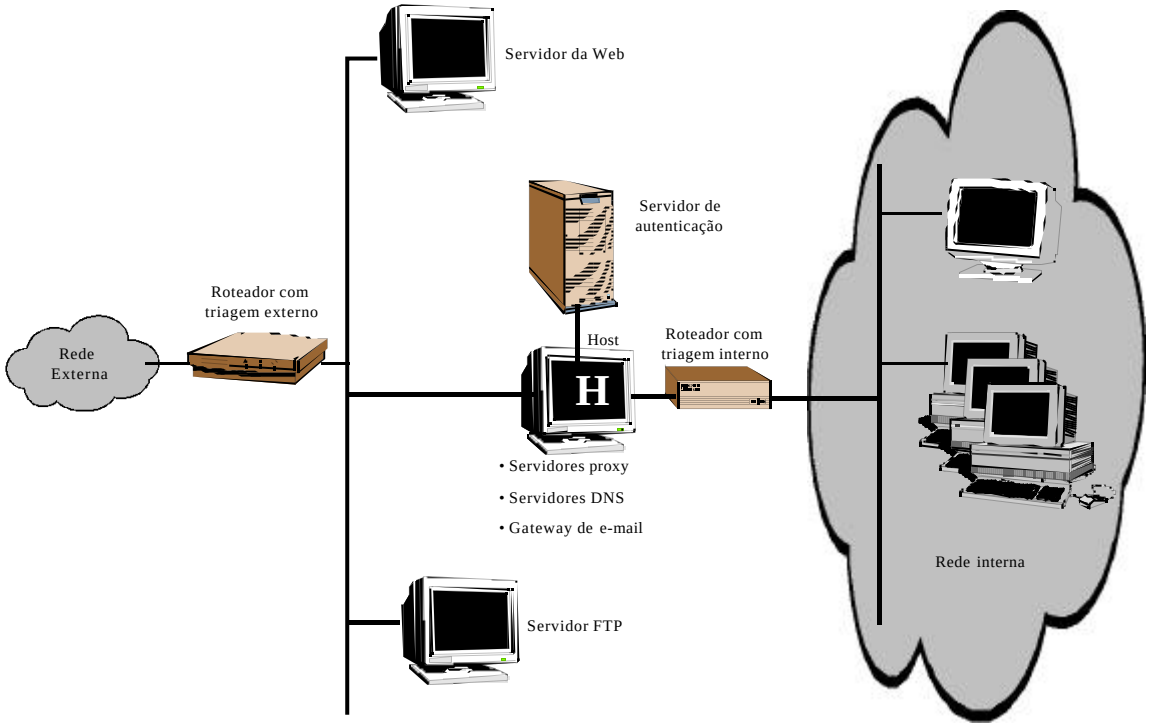

Figura 6 – *Belt and suspenders.*

4.4.6 - Componentes de um firewall

É fundamental desenvolvermos um conjunto de pré-requisitos que possa ser comparado a uma determinada solução. Esses pré-requisitos provavelmente serão específicos para cada empresa, mas há algumas diretrizes gerais para os elementos que deverão existir em um sistema de firewall robusto:

- Autenticação. São inúmeras as vantagens da autenticação rigorosa usando senhas e/ou cartões de token. Se já foi escolhido um padrão de autenticação para a empresa será necessário que o firewall seja compatível com esse mecanismo de autenticação.
- Controle de acesso**.** Até mesmo o filtro de pacotes mais simples oferece um controle de acesso baseado em endereço IP. Entretanto, muitas organizações podem

optar por restringir o acesso à Internet a usuários específicos (ou permitir apenas que determinados usuários acessem a rede remotamente via Internet) e exigir uma função mais rigorosa do que o controle de acesso simples baseado em endereços. Embora muitos disponham de recursos de controle de acesso e de autenticação baseados no usuário, talvez as grandes organizações tenham a expectativa de manter em um host de firewall contas de usuários individuais e perfis de acesso referentes a milhares de usuários.

- Compatibilidade com aplicações**.** Fundamentalmente, um firewall deve ser compatível com todas as aplicações que uma empresa deseja utilizar através da Internet. Para aplicações como telnet e FTP essa compatibilidade é direta: somente o mais inútil dos firewalls não é compatível com esses protocolos simples. A compatibilidade com proxies HTTP é menos importante: no entanto, sempre é possível usar um servidor da Web como um proxy HTTP nesse meio tempo. Um bom firewall também deve ser compatível com outros protocolos, incluindo protocolos store-and-forward, como o Netnews e o SMTP, e outros protocolos menos conhecidos, que a organização resolva utilizar. Além disso, um bom firewall deve incluir algum tipo de proxy de circuito, ou um “packet relay” genérico para TCP.
- Auditoria**.** O tipo de log de evento oferecido pelo sistema é de grande importância no contexto da administração contínua de um firewall.

Um bom firewall também deverá incluir alguma forma de “redutor” ou “divisor” de log, que seja capaz de acrescentar alguma inteligência ao processo de log, e também de tomar alguma providência caso um determinado evento ocorra (como, por exemplo, acionar o administrador através de um sistema de pager).

- Intangíveis. Muitas outras questões de natureza mais subjetiva podem ser levadas em consideração na avaliação de um firewall.

Alguns exemplos dessas questões são:

- Flexibilidade;
- Facilidade de uso;
- Compatibilidade com plataformas específicas;
- Ferramentas de administração;
- Suporte técnico;
- Custo.

Considerando a existência de grande número de fornecedores no mercado mundial e o caráter recente da tecnologia, avaliar produtos de firewall pode ser muito difícil. Para ajudar as empresas a tomar boas decisões, no final de 1995 um grupo de fornecedores reuniu-se para formar o Firewall Product Developers Consortium (FWPD), com o intuito de oferecer um conjunto de diretrizes para avaliar firewalls e para manter o público em dia com os novos produtos desenvolvidos nessa área.

4.4.7 - Princípios do projeto de firewall

Um dos primeiros princípios a serem considerados é que um firewall deve reforçar a política da organização. Daí a importância de identificar quais serviços terão permissão de cruzar uma conexão com a Internet em cada direção. Essa política tem duas filosofias conflitantes associadas a ela, a primeira, em geral conhecida como “tudo o que não for explicitamente negado é permitido”, adota uma estratégia aberta com relação à Internet. Apesar de ser extremamente amigável, essa filosofia deixa uma organização aberta a ataques com protocolos e serviços desconhecidos. Geralmente, no ambiente empresarial moderno, essa não é considerada uma política de conexão válida.

A instância mais comum é adotar uma política que afirma que “o que não for explicitamente permitido é proibido”. Apesar de talvez os usuários considerarem essa política um tanto draconiano, ela realmente representa uma forma efetiva de proteger uma rede contra ataques imprevistos. Além disso, essa filosofia deve transparecer em todas as partes da conexão com a Internet - a menos que ele seja explicitamente permitido, não deve haver forma alguma de o tráfego encontrar uma passagem para dentro da rede, depois que as decisões sobre a política tiverem sido tomadas e que o processo de projeto tiver começado, o projetista deverá manter quatro pontos em mente:

- **Usar componentes simples e bem definidos**. Um firewall executa diversas funções proxy de aplicação, servidor autenticação, servidor de nomes e monitor de tráfego, para citar algumas delas - e cada uma deve ser claramente definida e desempenhada por um componente do firewall. Ao adotar esse enfoque modular para a construção do firewall, sua organização encontrará mais facilidade na elaboração do firewall de acordo com as necessidades da empresa. Além disso, os componentes devem ser o mais simples possível. Se uma máquina funciona apenas como servidor DNS, ela não precisa executar um servidor de FTP ou de telnet. A presença de serviços

não utilizados não tem propósito e com freqüência cria pontos vulneráveis desconhecidos.

- **Usar ferramentas conhecidas e confiáveis**. Todos os dias, uma pessoa ou uma organização disponibiliza uma ferramenta de segurança na Internet. Deve-se tomar muito cuidado para assegurar a integridade dessas ferramentas e verificar sua origem.
- **Criar vários pontos de falha**. Esse conceito, as vezes denominada “defesa em profundidade”, tem como objetivo assegurar que o sistema de firewall não tenha um único ponto de falha. Mesmo que a consolidação dos componentes de um firewall em um único sistema possa economizar recursos, ela resulta na concentração de muitas responsabilidades em uma única máquina. Se essa máquina falhar ou for comprometida, toda a rede também poderá ser comprometida. A conclusão disso tudo é que devem-se usar produtos de vários fornecedores em um firewall (como roteadores Cisco e Bay Networks). Dessa forma, se uma falha for encontrada no produto ou no sistema operacional de um dos fornecedores, somente parte do sistema correrá risco.
- **Prestar atenção aos modos de falha**. Os firewalls devem ser construídos de modo a serem à prova de falha - ou seja, se a máquina falhar, for reinicializada, ou travar, a atitude padrão deverá ser *impedir a passagem do tráfego,* em vez de permiti-la, mesmo que o tempo de inatividade seja longo, acreditamos que essa opção é preferível à outra, na qual qualquer um tem acesso à rede da corporação. Uma maneira simples de aperfeiçoar o modo de falha de um sistema é confirmar que os mecanismos de segurança das máquinas do firewall estão configurados e ativos antes de a interface de rede ser criada. A razão para essa estratégia reside no fato de que se o mecanismo de segurança não carregar, a interface da rede não pode ser ativada sem o mecanismo de segurança auxiliar.

4.4.8 - Questões de implementação

Uma coisa é escolher e instalar um firewall, outra muito diferente é ter a tranqüilidade de saber que ele foi instalado corretamente e está funcionando da maneira esperada. Basicamente temos três maneiras muito fáceis de verificar e testar a integridade de um sistema de firewall: listas de verificação, ferramentas e testes independentes.

- **Listas de verificação**. As listas de verificação são projetadas para assegurar que nenhuma área do sistema tenha sido esquecida, e para garantir proteção contra falhas humanas. Apesar de haver inúmeras listas de verificação disponíveis tanto em fontes públicas como através de consultores de segurança profissionais, a relação a seguir engloba as áreas mais importantes que as listas de verificação devem incluir:
    - Política. A implementação do firewall reflete de maneira adequada à política de empresa com relação à Internet?
    - Configuração dos Filtros de Pacotes. Os roteadores ou outros filtros de pacotes estão configurados de modo a utilizar o mais simples conjunto de regras necessárias?
    - Controle de Acesso aos Sistemas. O acesso a todos os sistemas "bastion hosts" é controlado através de algum outro recurso além de uma simples combinação de identificação/senha do usuário?
    - Controle de Acesso aos Roteadores. O controle de acesso aos roteadores é limitado ao acesso por terminal? Como alternativa, um protocolo de autenticação (como o TACACS) é usado para controlar o acesso ao roteador? O roteador impõe limitações sobre quem pode enviar a ele atualizações de roteamento? SNMP? ICMP?
    - Configuração dos Serviços da Internet. Todos os serviços externamente disponíveis estão configurados de maneira segura?
- **Ferramentas**. Muitas ferramentas de segurança de rede podem auxiliar no processo de verificação, principalmente em relação àquelas organizações que desejam mais uma verificação verbal do firewall. Essas ferramentas, incluindo o PINGWARE da Bellcore, o NetProbe da Infostructure, o Internet Security Scanner da ISS e até o infame SATAN, podem ser eficientes na descoberta de falhas em sistemas. Além disso, algumas ferramentas de verificação de firewalls estão em desenvolvimento. Em sua maioria, essas ferramentas monitoram passivamente o tráfego nos dois lados do firewall, para verificar o tipo de tráfego que flui. Esse tráfego é comparado com a política de empresa, e qualquer discrepância aciona um alarme. Muitas outras ferramentas também podem ser configuradas para gerar um tráfego de teste que ajuda nesse processo.

- **Testes Independentes**. Existem empresas cujas principais atividades são o teste e a verificação de firewalls. Essas empresas vão até seu site, tentam encontrar falhas no seu firewall e relatam o que encontram. Em geral, essas verificações são de dois tipos. Um exercício comum é uma verificação geral da segurança da rede, na qual o consultor utiliza listas de verificação, ferramentas de verificação e faz uma inspeção para ver se as idéias por trás do projeto e da implementação do firewall são sólidas e foram corretamente aplicadas.

Um exercício mais criterioso (e que achamos mais informativo) é um teste de invasão real. Nesse tipo de teste, o consultor tenta invadir o perímetro da sua rede a partir de um site externo. Esse teste de invasão é projetado para formular um ataque verdadeiro por parte de um hacker tentando invadir a rede, e deve utilizar todas as ferramentas disponíveis para a comunidade de hackers. Testes de invasão podem ser a maneira mais eficaz de verificar um sistema de firewall e são a alternativa "segura" mais próxima de um ataque real. A administração do firewall é um processo contínuo. O administrador deve ter conhecimento e experiência no campo de segurança na Internet. No entanto, se essa pessoa deixar a empresa, alguém deverá estar pronto para assumir a função o mais rápido possível. Um guia do administrador de firewall que possa ser entregue ao novo administrador é particularmente útil.

Esse guia deverá tratar dos seguintes assuntos:

- A política da organização para a Internet;
- Como conceder ou revogar o acesso dos usuários à Internet;
- Como modificar as regras existentes conforme necessário;
- O que fazer em caso de invasão;
- Como prover a segurança das máquinas novas quando forem instaladas;
- Procedimentos para a leitura e a revisão dos logs;
- Procedimentos para a distribuição dos cartões de token aos funcionários.

É igualmente importante estabelecer alguns procedimentos para a geração de logs do tráfego na conexão à Internet. Tanto do lado de dentro quanto do lado de fora do firewall. E certo que os logs podem ser muito úteis (se forem lidos), mas eles também podem ser prolixos. Além disso, os logs tendem a ser uma reação ao problema - ninguém os lê até algo acontecer. A maioria dos produtos de firewall vem com algum

tipo de mecanismo de log, mas muitos não têm qualquer “redutor” ou inteligência que possa extrair do log os fatos interessantes e que causam preocupação.

Firewalls vêm protegendo redes locais privadas de intrusos hostis a partir da Internet, de modo que o número de LANs hoje conectadas a Web é muito maior do que se esperaria, dados os riscos de segurança envolvidos. Estes sistemas permitem aos administradores de redes oferecer acesso a serviços específicos da Internet a usuários internos selecionados, como parte de uma política de gerenciamento de informação que envolve não apenas a proteção da informação interna como também o conhecimento de quem acessa o quê na Web. Não há uma única resposta à pergunta "qual é a melhor solução de projeto de firewall para redes?". A decisão por uma ou outra arquitetura dependerá de diferentes fatores, como a política de segurança global da organização, o conhecimento técnico do pessoal que administra as soluções empregadas, o custo e o nível percebido de ameaça externa. A melhor solução conjugará estes fatores também com os requisitos de serviços a oferecer externamente e aos usuários internos e o grau de dificuldade no acesso que se imporá a estes.

4.5 – DICAS PARA AJUDAR A PROTEGER SEU NEGÓCIO

4.5.1 O caminho da segurança

Existem pontos que são básicos na estruturação de uma solução de segurança. A base para qualquer tomada de decisão deve ser a necessidade de negócios da corporação. É exatamente isso que vai definir quais informações poderão ou não ser expostas. Depois de verificar quais dados e processos são importantes para o negócio, é necessário fazer uma analise da tecnologia e de como ela está sendo usada, além de levantar as vulnerabilidades e riscos. A partir dessas informações é possível elaborar e determinar uma política de segurança. Esta política de segurança pode ser aberta (tudo que não é proibido é permitido) ou fechada (tudo que não é permitido é proibido).

Definido tudo o que será permitido ou proibido, então é que se parte para definição do modelo de segurança. Nessa fase, definem-se as responsabilidades de usuários, qual tecnologia será utilizada. Dai a importância de se ter à política de segurança primeiro, porque é essa política que vai nortear a tomada de decisões.

Mas a tarefa não termina com a implantação de produtos. Em seguida, é necessário definir como será feitos a administração dessa estrutura e comunicar as diretrizes e procedimentos para os usuários finais. Boa parte dos problemas é possível de resolver somente com a conscientização dos usuários. Manter uma equipe interna de segurança ainda é muito caro. Isso porque são poucos os profissionais preparados e a necessidade de treinamento é constante. Neste caso, a opção pode ser a terceirização de algumas atividades e manter pelo menos um técnico especialista na empresa. Tendo em vista a necessidade de se estar sempre monitorando os acessos e possíveis falhas na rede, para fortalecer as barreiras contra os invasores.

4.5.2 13 etapas de uma política de segurança, que podem ser fundamentais na proteção do seu negocio.

4.5.2.1 – Conscientização: é fator crítico de sucesso conseguir o comprometimento dos altos executivos e não menos importante preparar as pessoas para a mudança de cultura. Seminários de conscientização, onde se explica a importância da segurança e o papel das pessoas no cenário corporativo são fundamentais.

4.5.2.2 – Análise do negócio: é preciso analisar o paciente antes mesmos de receitar qualquer medicamento. O mesmo se pode dizer da empresa. A solução de segurança tem de visar o negócio e não somente ambientes processos e tecnologias isoladas. Mesmo que não se possa implementar simultaneamente em toda a empresa, é necessário que os projetos se encaixem e estejam bem definidos em um amplo plano diretor de segurança. A analise do negócio deve acontecer através de entrevistas, onde se pode levantar a competência básica, a cultura da empresa, o fluxo de informações, os processos críticos e conseqüentemente os ativos (infra-estrutura, aplicações, processos e pessoas) merecedores de uma analise mais profunda.

4.5.2.3 – Analise das vulnerabilidades: dando continuidade essa fase permitirá identificar as vulnerabilidades e priorizá-las de acordo com a crticidade. A análise do ambiente predial permitirá o conhecimento dos aspectos físicos da segurança no que diz respeito a incêndio, instalações elétricas, cabeamentos lógicos, condições climáticas e

controle de acesso físico seguindo o conceito de perímetros de segurança. A análise de documentos é importante para que políticas corporativas, especificações técnicas, regras de configuração de ambiente e até mesmo normas de qualidade sejam levadas em consideração. A análise do ambiente informatizado é a fase complementar. Servidores, estações de trabalho, firewalls, roteadores, switches, links e equipamentos de conectividade em geral são analisados tecnicamente a procura de vulnerabilidades que potencializem as ameaças.

4.5.2.4 - Normas de segurança: - esquecidas por muitas empresas, as normas de segurança talvez seja um dos fatores mais importantes para garantir a segurança corporativa. Isso porque ele trata justamente do ativo mais esquecido: as pessoas. É o conjunto formado por diretrizes, normas, procedimentos e instruções que irá nortear os usuários quanto ao uso adequado dos recursos a eles disponibilizados. É onde se definem regras, comportamentos, proibições e até punições por má utilização dos recursos disponíveis. Este documento igualado com as devidas proporções à importância da constituição de um país, tem de ser escrito sob medida. Deve estar de acordo com a cultura da empresa e seus recursos tecnológicos, para então, ser seguido e não apenas representar um grande volume de papel empoeirado e esquecido em algum canto. Regras de manutenção e criação de senhas, rotinas de backup, fragmentação de material descartado, limites para uso de e-mail e a definição de trilhas de auditoria são alguns dos pontos abordados.

4.5.2.5 - Classificação da informação: complementado as normas de segurança, a classificação da informação é responsável por descrever os procedimentos para seleção, manipulação, transporte, armazenamento e descarte de informações, identificando-as de acordo com sua importância. Com base no perfil do negócio e característica das informações que circulam no ambiente corporativo, se estabelece um padrão de classificação como, por exemplo: confidencial, restrito, interno e para divulgação. Desta forma todos saberão como se comportar diante das informações que manipulam

4.5.2.6 - Campanha de divulgação: com as pessoas conscientizadas pelos seminários e as normas de segurança elaborada, surgem uns novos desafios: fazê-las seguir o que

foi definido. Pensando justamente em tornar essa tarefa mais fácil, as campanhas de divulgação segmentam todo o enorme conteúdo da política de segurança, focando nas normas, procedimentos e instruções ligadas ao dia-a-dia de cada departamento da empresa. As pessoas passam então a receber informação filtrada, o que certamente trará eficiência. Cartazes nos corredores e e-mails informativos completam a iniciativa.

4.5.2.7 - Implementação da segurança: chegou à hora da verdade. Depois de conhecer as vulnerabilidades, agora priorizadas por criticidades (impacto vs. Risco), cruzadas com as necessidades inerentes a cada ambiente e a atividade do negócio, aplica-se soluções de hardware e software, um vasto leque de ferramentas que se integram, que garantirão o nível de segurança. Antivírus, hot-fixes e patches de correção de sistemas operacionais, certificados digitais, salas-cofre, criptografia, smart-card, software de intrusion detection, virtual private network, roteador, firewall e aplicações Public Key Infrastruture, são algumas das soluções pontuais que podem compor o ambiente. Aplicação da política de segurança em português faz parte da implementação de segurança. Software que seguem critérios predefinidos, de utilização dos recursos tecnológicos, seja nos servidores ou estações de trabalho, e até mesmo uma equipe de auditoria, podem ser os responsáveis pelo sucesso da adesão das pessoas às diretrizes, normas, procedimentos e instruções que regem a política de segurança. Agir com transparência se for aplicar tais recursos, afinal você deseja que seus funcionários sejam seus aliados.

4.5.2.8 - Termo de sigilo: questionado por muitos e aplicados por alguns, o termo de sigilo representa um pacto de compromisso entre a empresa e o funcionário no que tange o uso correto dos recursos tecnológicos a ele disponibilizados. Não existe um respaldo legal, mas já é uma iniciativa de comprometê-lo com o sucesso da empresa na integração entre tecnologia e negócio. Seu sucesso está diretamente ligado conscientização comentada na primeira fase.

4.5.2.9 - Teste de invasão: tem seu importante papel pondo à prova, com a segurança assegurada por um especialista, o ambiente corporativo ao utilizar as técnicas e ferramentas mais difundidas. Software de sniffer (grampo digital), trojan horses

(cavalos de tróia), transhing (análise de lixo) e engenharia social são terminologias dessa etapa.

4.5.2.10 - Plano de contingência: garantir a continuidade de processos ou informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre. Com este propósito e formado pelas etapas: estratégias de contingências, planos de retorno e os procedimentos de contingência propriamente ditos, o plano de contingência de ser escrito para ser verdadeiramente executado, portanto, deve ser realista. Janela de tempo, tolerância à paralisação, gatilhos de acionamento e rotas alternativas de comunicação são alguns dos parâmetros analisados.

4.5.2.11 - Administração de segurança: a busca pela segurança deve ser uma atividade constante, afinal quando uma nova tecnologia se incorpora ao ambiente corporativo, nova vulnerabilidades acompanham. Desta forma, as macros etapas: análise, política e implementação, devem ser refeitas visando à atualização. Segurança é um processo cíclico.

4.5.2.12 – Oficial de Segurança (Security Officer): expressão nova para muitos, mas já uma realidade para as empresas modernas, o Security Officer é um cargo, uma ocupação cada vez mais importante. A segurança eletrônica é percebida como fator crítico de sucesso e por isso precisa ser planejada e coordenada por quem realmente a tem como competência básica. Alguém que pense em segurança o tempo todo e que acompanhe a evolução tecnológica, reduzindo o tempo de defasagem entre a descoberta de uma nova vulnerabilidade e sua solução.

4.5.2.13 - Solução corporativa de segurança da informação: pense no negócio e não apenas em soluções pontuais. Deve-se traçar uma estratégia focada na busca da segurança eficiente, tendo em vista as dificuldades de se acompanhar o surgimento de novas formas de invasão que os intrusos criam para ter acesso e burlar as informações corporativas de uma entidade, esse risco aumenta na medida que cresce o uso da tecnologia na corporação.

CONCLUSÃO

Hoje em dia tudo gira em torno dos computadores, pela agilidade que oferece na execução das tarefas dentro de uma instituição, por isso esta obra não se destina somente àqueles envolvidos diretamente no mundo dos bits e dos bytes, mas também ao empresário que tem sua empresa informatizada e que é de extrema necessidade, proteger suas informações como sendo um bem valioso, que são determinantes nas decisões estratégicas dos negócios, devido à maneira rápida como a Internet tomou conta de nossas vidas e mudou completamente a forma de se ver o mundo, seja no ambiente de trabalho ou em casa, pois todos estarão diretamente ligados ao mundo inteiro a partir do momento em que se desejar, para isto basta ligar o computador, ou seja plugar o mesmo em uma telefônica através de uma placa de modem e pronto, a partir deste momento entra-se em contato com a maior fonte de informações do planeta, a World Wide Web.

Atualmente para tudo o que se pensa fazer pensa-se em sentido mundial, existe uma visão globalizada seja nos negócios ou no cotidiano particular e o mundo a cada dia que passa volta-se cada vez mais a integralização de todos, e a Internet foi somente um dos meios utilizados para tornar essa maneira de pensar em realidade. E com certeza isso ainda vai chegar a um ponto de não precisar sair de casa para resolver um problema bancário de qualquer ordem ou complexidade, ir ao dentista ou médico para uma simples consulta, ao supermercado e outras coisas banais. Mais isso só será possível na medida em que os sistemas tornarem-se mais seguros e melhor controlados em prever um ataque antes que haja a invasão. O fator de risco se agrava quando estas invasões são feitas em grandes empresas que gastam milhões em sistemas de segurança, e esse costume começa a disseminar-se com mais freqüência, gerando perdas anuais de milhões de dólares. Mas com o tempo, as coisas mudam: os Administradores mudam ou assumem novas responsabilidades, o perfil de utilização da Internet muda, os softwares de segurança são acionados para fazer mais do que o previsto inicialmente, ou seja, somente evitar que usuários não autorizados acessem a rede interna. Para verificar se tudo ainda está funcionando bem muitas empresas optam por ter verificações e/ou testes de invasão realizados periodicamente.

Além disso, com o passar do tempo, será necessário reavaliar o objetivo das ferramentas (software e hardware). Se sua empresa estiver criando um site na Web que será visitado por milhares de pessoas por dia, você provavelmente desejará abandonar o roteador com triagem e pensará em substituí-lo por algo que disponha de recursos de log e um melhor controle de acesso. Pois, um Software de proteção bem configurado pode ser um componente extremamente útil em uma solução para segurança na Internet, quase sempre representando a diferença entre a defesa bem-sucedida de uma rede e uma manchete de primeira página. No entanto, os softwares de segurança são apenas parte da história. A outra fica por conta dos Administradores da rede para implantar uma política de segurança na empresa a fim de mostrar a todos os perigos que existem dentro e fora da empresa.

Tudo isso para melhorar o funcionamento operacional, evitar invasões e adequar as atividades da empresa às novas aplicações propostas de forma protegida.

BIBLIOGRAFIA

Caruso e Steffen, CARUSO, Carlos A. A. e STEFFEN, Flávio D. *Segurança em informática*. LTC – Livros Técnicos e Científicos Editora, 1991.

Bernstein, 1996, BERNSTEIN, Terry and others. *Internet security for business*. John Wiley & Sons, Inc, 1996.

Chapman e Zwiciky, CHAPMAN, D. B. & ZWICIKY, E. D. *Building internet firewalls.* O'Reilly & Associates, Inc, 1995.

Amoroso and Sharp, AMOROSO, Edward and SHARP, Ronald. *PCweek intranet and internet firewall strategies.* Ziff-Davis Press, an imprint of Macmillan Computer Publishing USA, 1996.

Alexander, ALEXANDER, Michael. *Net security: your digital doberman.* Ventana Communications Group, Inc, 1997.

Schneier, SCHNEIER, Bruce. *Applied cryptography - second edition.* John Wiley & Sons, Inc, 1996.

Cobb, COBB, Stephen. *NCSA firewall policy guide*. National Computer Security Association, v 1.01, 1996.

Outros, ARNETT, M. F. e Outros. *Desvendando o TCP/IP***.** Editora Campus Ltda. Rio de Janeiro, 1997.

Strark, Thom. *Criptografia para um planeta pequeno*. Byte Brasil. Editora Rever Ltda, 6(03) : 16-19, março, 1997.

Augusto, Alexandre e WAYNER, Peter. *Cuidado! o seu cofre está aberto.* Byte Brasil. Editora Rever Ltda, 6(06) : 46-69, junho, 1997.

Ribeiro, Gisele. *As suas informações estão seguras?* Byte Brasil. Editora Rever Ltda, 6(11) : 66-74, novembro, 1997.

Tunnel, AltaVista. *Administrator's Guide.* Digital Equipment Corporation. Maynard, Massachusetts, 1998.

Firewall, AltaVista. *Administrator's Guide.* Digital Equipment Corporation. Maynard,

Lopes, Fábio. A fortaleza dos Negócios. Network Computing, Brasil, nº. 12, (01): 29-34, fevereiro 2000.

Sêmola, Marcos. Analisando Vários Tópicos na Política de Segurança. Developers Magazine, Brasil, nº 54 (05): 10 – 13, fevereiro 2001.

Grego, Mauricio. Harcker como eles atacam. Info exame, Brasil, nº 179 (16): 34-39, fevereiro 2001.

Junior, Roberto Cury; CAVALHEIRO, Tony. Conhecendo o Mundo dos Harckers. PC Máster, Brasil, nº 5, v. 41 (4): 26 – 41, Outubro 2000.

Starlin. GORKI. Manual Completo do Harcker. Editora Book Express. Rio de Janeiro 1999.

Anchieta, Olavo. ANCHIETA, Olavo José Gomes. Segurança Total. Editora Makron Books do Brasil Ltda. São Paulo 2000.