RICARDO AUGUSTO GARCIA

SERGIO HIDEO HIGASHI

SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA DA INFORMAÇÃO

MONOGRAFIA DE CONCLUSÃO DO
CURSO DE ESPECIALIZAÇÃO EM
TECNOLOGIA DA INFORMAÇÃO – MTI

ESCOLA POLITÉCNICA DA USP

São Paulo

2002

RICARDO AUGUSTO GARCIA

SERGIO HIDEO HIGASHI

SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA DA INFORMAÇÃO

MONOGRAFIA DE CONCLUSÃO DO
CURSO DE ESPECIALIZAÇÃO EM
TECNOLOGIA DA INFORMAÇÃO – MTI

ESCOLA POLITÉCNICA DA USP

ÁREA DE CONCENTRAÇÃO:
ENGENHARIA DE COMPUTAÇÃO
E SISTEMAS DIGITAIS

ORIENTADORA:
PROF. DRA. GRAÇA BRESSAN

São Paulo
2002

RESUMO

Este trabalho tem o objetivo de apresentar soluções e ferramentas tecnológicas que poderão ser usadas como parte de uma implementação de um projeto de segurança ditada por uma política bem definida para garantir o cumprimento dos três pilares da segurança da informação, a confidencialidade, a integridade e a disponibilidade.

Na introdução, são colocadas considerações gerais sobre os problemas que a "globalização" da informação, através da Internet, trouxeram em paralelo aos inegáveis benefícios para a sociedade, civil e corporativa, mas que tornaram o ambiente de tecnologia da informação bastante vulnerável às inúmeras ameaças do mundo virtual.

Em seguida é apresentada a norma ISO/IEC 17799, um documento com recomendações contemplando as melhores práticas em segurança e que deve ser seguida como base para a implementação de um projeto de segurança.

Os principais problemas de segurança são relatados com estatísticas mais recentes sobre as suas ocorrências e com alguns números e informações para ilustrar as suas graves conseqüências.

Como objeto do trabalho, no capítulo 3 são relacionadas as principais ferramentas, software ou hardware, que eliminam ou minimizam os problemas relacionados.

No capítulo 4 conclui-se com recomendações e cuidados a serem tomados para a implementação parcial ou total dessas ferramentas num projeto de segurança, decisão que deve levar em conta os maiores riscos aos negócios da empresa.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ADSL - Asymmetric Digital Subscriber Line

ATM - Asynchronous Transfer Mode

AT&T - American Telephony & Telegraphy

B2B - Business to Business

CESP - Companhia Energética de São Paulo

CPU - Central Processing Unit

CSI/FBI - Computer Security Institute / Federal Bureau of Investigations

CTEEP - Companhia de Transmissão de Energia Elétrica Paulista

DNS - Domain Name System

E/S - Entrada / Saída

FTP - File Transfer Mode

ICMP - Internet Control Message Protocol

IEEE - Institute of Electronical and Eletrotechnical Engeneers

IRC - Internet Relay Chat

NAI - Network Associates Inc

NFS - Network File System

ISO/IEC - International Standardization Organization /

NTP - Network Time Protocol

POP - Post Office Protocol

RAS - Remote Access Server

RPC - Remote Procedures Call

1 INTRODUÇÃO

A partir de meados da década de 80, com a popularização dos microcomputadores, iniciou-se uma mudança radical na forma de acessar e tratar as informações no mundo empresarial. Até então, as informações e os sistemas centralizados no chamado mainframe eram compartilhados e disponibilizados através das redes de terminais que, simplesmente, apresentavam as informações basicamente como as recebiam, por isso conhecidos como terminais de vídeo ou não inteligentes, sem capacidade de processamento próprio. Na maioria dos casos, a chamada rede de teleprocessamento que conectava aqueles terminais era propriedade da empresa que mantinha toda a infraestrutura necessária para a sua operação e interligando somente suas próprias unidades.

A figura 1 apresenta uma configuração de rede típica da época, quando se tinha, no máximo, conexões externas através do protocolo x.25 e os primeiros microcomputadores (personal computer) com sua capacidade ainda limitada emulando terminais de vídeo através de placa específica para esse fim e, quando muito, para transferência de arquivos de e para o mainframe.

Visão Geral – Antes

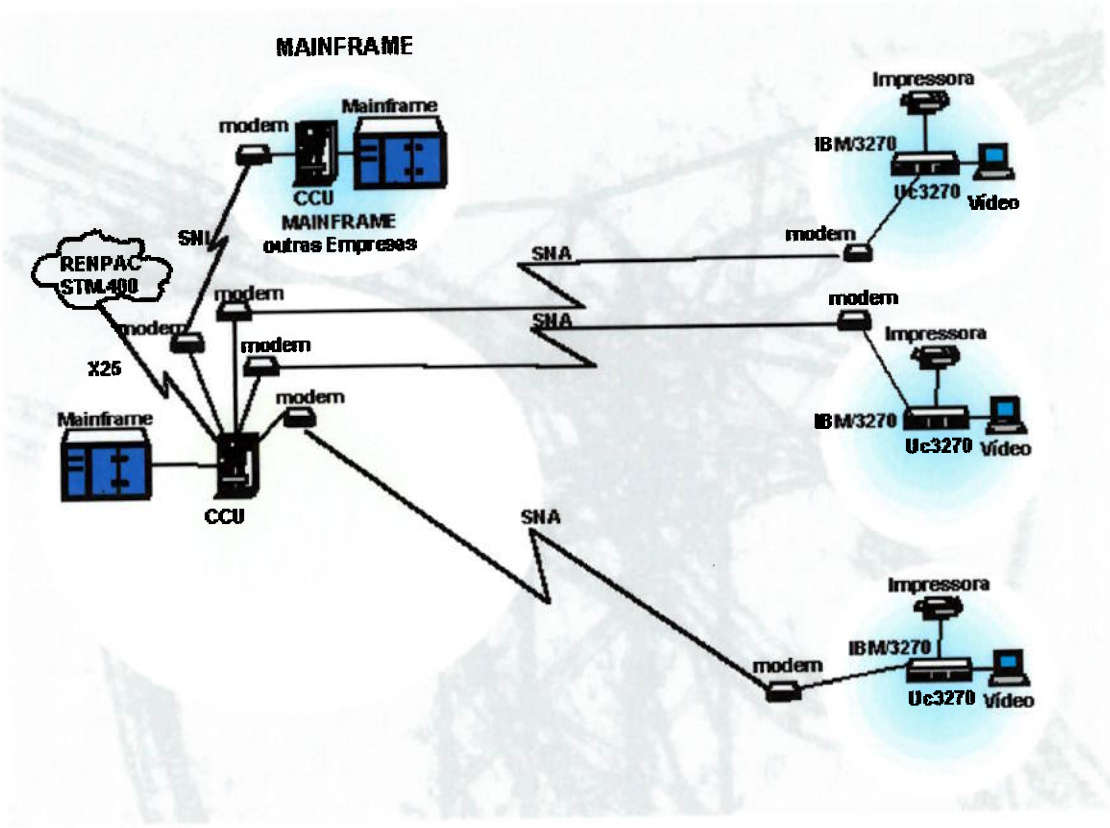

Figura 1 - Configuração típica das primeiras redes

Fonte: Documentação de rede da antiga CESP

Com o advento da Internet, novamente grandes mudanças, até de hábitos, ocorreram tanto no que se refere à comunicação interpessoal/empresarial quanto no modo de negociar das empresas, das pequenas às grandes corporações.

No âmbito pessoal o grande sucesso deste recurso deve-se à sua facilidade de uso e, talvez principalmente, pela ausência de regras para a sua utilização, num ambiente de grande permissividade. Em termos empresariais, o avanço tecnológico dos meios de comunicação e a contínua queda de custo de sua contratação, o enorme público potencialmente consumidor, as facilidades de interconexão de redes locais ou geograficamente distantes entre outras razões, fizeram com que mais e mais empresas também aderissem aos encantos da rede mundial. Neste cenário, a dificuldade de se manter infra-estrutura própria provocada pelos custos e pela necessidade de constante especialização principalmente na tecnologia de interconexão de redes e, por outro lado, pelos benefícios decorrentes da agressiva

concorrência entre os fornecedores desse tipo de serviço levaram as empresas à prática de terceirização, o que as levou a perder parcialmente o controle sobre o tráfego das informações que tinham até então; hoje, verifica-se a terceirização em praticamente todo tipo de atividade no ambiente da tecnologia da informação.

Visão Geral – Atual

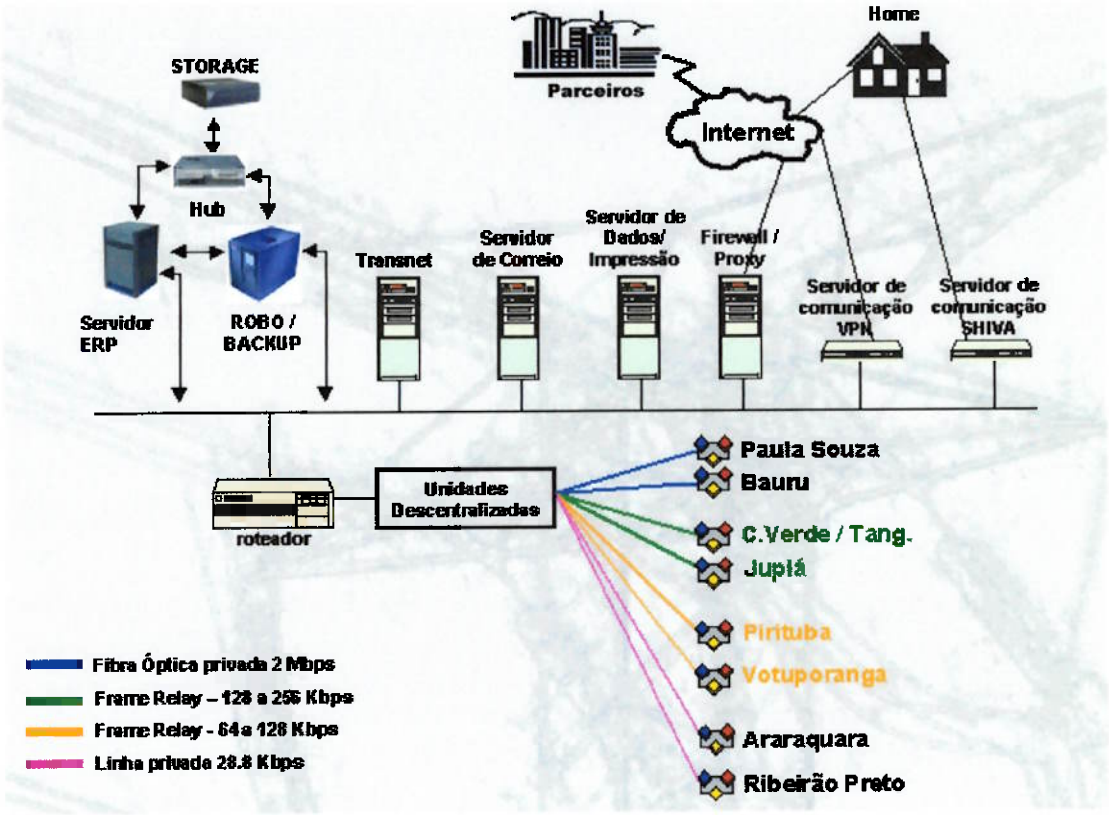

Figura 2 - Configuração típica de uma rede atual

Fonte: Documentação de rede da CTEEP

A figura 2 representa uma típica rede atual, que comparada à da figura 1 evidencia a evolução ocorrida nesses poucos anos.

Revolucionando costumes ou rompendo barreiras geográficas, a Internet tornou todo tipo de processo mais ágil e, consequentemente, aumentou a produtividade de pessoas e empresas. Entretanto, à medida que mais e mais pessoas e empresas totalmente heterogêneas em termos de comportamento e de infraestrutura tecnológica se conectavam à rede mundial, a complexidade para se manter a "convivência" e a conectividade dessa heterogeneidade aumentou tanto que aos poucos foram se

descobrindo brechas e falhas ou fragilidades que acabaram gerando possibilidades para que pessoas mal intencionadas se aproveitassem para criar situações, caracterizadas desde a simples necessidade de "promoção" pessoal até aquelas para benefício próprio através da posse deliberada de "propriedades" alheias, que tornaram esse mundo totalmente inseguro.

No mundo corporativo, essas falhas têm conseqüências ainda mais danosas potencializadas pela cultura dos empregados com relação à segurança, traduzida em vícios e negligências. Soma-se a isso o perigo real decorrente de empregado insatisfeito e, não raro, com permissões indevidas de acesso à informações críticas da empresa. Segundo um dos resultados da "Oitava Pesquisa Nacional sobre Segurança da Informação" desenvolvida pela Módulo Security Solutions S.A. através da análise das respostas de 547 questionários coletados entre março e agosto de 2002 , junto a profissionais ligados à área de tecnologia e Segurança da Informação de diversos segmentos de negócios, a principal ameaça às informações conforme mostrado na figura 3 foi apontada como sendo de funcionário insatisfeito; citados também como grande ameaça a divulgação de senhas, o vazamento de informações, super poderes de acesso e o uso indevido de recursos entre outros que se podem considerar conseqüência da citada cultura.

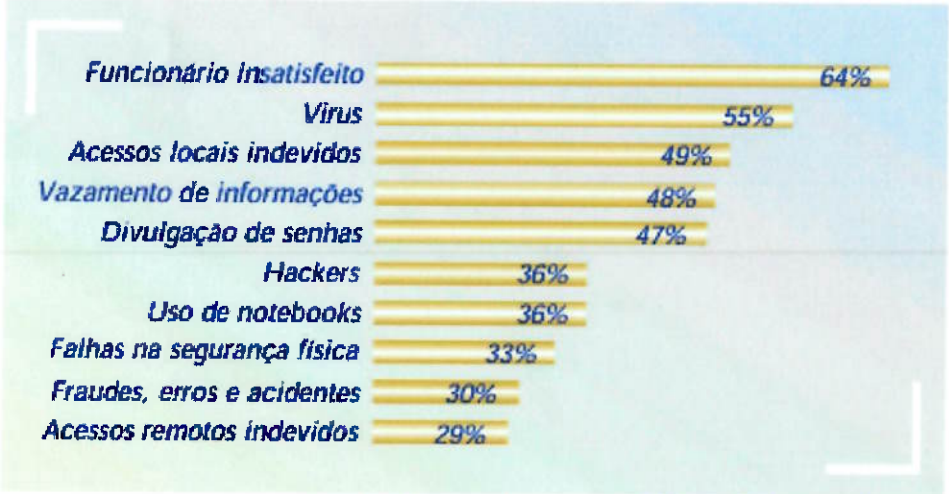

Figura 3 - Principais ameaças às informações da empresa

Fonte - 8° Pesquisa Nacional sobre Segurança da Informação [Módulo, 2002]

Ainda no ambiente corporativo, em contraste ao ganho de eficiência trazido pela Internet, há o lado negativo decorrente da má utilização desse recurso; empregados, mesmo durante o expediente, passam horas navegando pela rede mundial em buscas e pesquisas que nada tem a ver com o desenvolvimento do seu trabalho; em outra situação, o correio eletrônico é utilizado também para troca de mensagens pessoais totalmente dissociadas das atividades profissionais e, mais grave, para transmissão indevida de informações corporativas sigilosas, além do recebimento de indesejadas mensagens tais como os spams e aquelas com anexos infectados, intencionalmente ou não, por vírus.

Não se tratando mais de um diferencial de competição entre as empresas, a segurança da informação deve ser hoje vista como um requisito básico para a participação de empresas e até de pessoas no mundo Internet, requisito sem o qual não se garante a continuidade dos negócios e, na pior das situações, põe-se em risco a sobrevivência não só do negócio como da própria empresa. Mas independente de Internet, considerando que hoje a informação é tratada como um dos ativos mais importantes de qualquer organização, tratamento diferenciado deve ser dado ao projeto de segurança.

1.1 Objetivo do trabalho

Este trabalho tem o objetivo de apresentar soluções e ferramentas tecnológicas que contemplem a proteção contra as maiores ameaças à informação, como parte de uma implementação de um projeto de segurança ditada por uma política bem definida para garantir o cumprimento dos três pilares da segurança da informação, a confidencialidade, a integridade e a disponibilidade.

Existe farta bibliografia sobre as soluções tecnológicas. Entretanto, a maioria concentra-se num determinado produto/sistema e outras, apesar de mais abrangentes, também se detém a detalhes e tratados teóricos mais apropriados para a especialização de técnicos responsáveis por cada ramo de segurança. Este trabalho visa agrupá-las num só documento de forma mais acessível e compreensível para o nível de coordenação e gerencial responsáveis pela segurança corporativa da informação.

Considerando que a CTEEP gradativamente se abre para a rede mundial, seja para integrar e integrar-se a parceiros e prestadores de serviço visando o aumento da produtividade ou para facilitar o acesso dos seus empregados em trânsito ou de suas residências de forma consciente, responsável e segura, este grupo resolveu desenvolver este trabalho que poderá servir como subsídio na aquisição das soluções tecnológicas, o que deve ocorrer após a definição das políticas, da análise de vulnerabilidade da infra-estrutura atual e da análise de riscos aos ativos da empresa.

2 SEGURANÇA DA INFORMAÇÃO

2.1 Conceituação

O Decreto Federal nº 3505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal conceitua Segurança da Informação como sendo "a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento".

Com a definição acima, podemos dizer que a segurança da informação tem como objetivo:

- preservar a CONFIDENCIALIDADE da informação, de modo a garantir o seu acesso somente para pessoas devidamente autorizadas;
- garantir a INTEGRIDADE, ou seja, a exatidão das informações e dos métodos de processamento;
- manter a DISPONIBILIDADE, garantindo que os usuários autorizados tenham acesso à informação sempre que necessário.

O cumprimento dessas três bases clássicas de segurança deve ser obtida pelo conjunto de componentes constituídos de ferramentas que compõem a arquitetura tecnológica, das instalações físicas, de procedimentos e de pessoas.

2.2 Norma NBR ISO/IEC 17799

Um sistema de segurança da informação é tão mais eficiente quando planejada e implementada seguindo-se uma norma ou padrão. Para tanto, a norma NBR ISO/IEC 17799 "Tecnologia da Informação - Código de Prática para a Gestão da Segurança da Informação", um conjunto de controles organizados contemplando as

melhores práticas em segurança da informação e reconhecidas internacionalmente como padrão, facilita nesta tarefa e, se aplicada desde as fases iniciais do projeto e de especificação dos requisitos, garante não só a eficácia mas também um custo consideravelmente menor. A norma fornece uma base comum através de um conjunto de recomendações para a gestão da segurança para todos os envolvidos num projeto de segurança da informação corporativa.

Conforme a norma, a informação é um ativo que, como qualquer outro que seja importante para os negócios, tem um valor para a organização e, portanto, precisa ser adequadamente protegida contra as várias ameaças de modo a garantir a continuidade dos negócios, minimizar os danos, gerar novas oportunidades de negócio e maximizar o retorno dos investimentos.

A seguir são relacionados de forma resumida os tópicos que agrupam todos os controle da norma.

2.2.1 Política de Segurança

Este tópico descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança; cita a importância do estabelecimento, pela direção da empresa, de uma política clara e do seu comprometimento.

2.2.2 Segurança Organizacional

Este tópico aborda a estrutura de uma equipe gerenciada para o trato da segurança, com o estabelecimento de atribuições e responsabilidades, inclusive de contratados e prestadores de serviço.

2.2.3 Classificação e controle dos ativos

Este tópico agrupa os controles relacionados aos ativos da corporação. Estabelece que todos os ativos sejam inventariados e tenham um proprietário responsável. São considerados ativos as informações (base de dados, arquivos, documentações, procedimentos, etc...), software (aplicações, sistemas, utilitários), equipamentos (processadores, de comunicação, mídia, etc...) e os serviços (de comunicação, de utilidades gerais como refrigeração, eletricidade, etc...). Inventariados e valorados

esses ativos, tem-se uma idéia melhor dos riscos que se podem correr com os investimentos, normalmente escassos, a serem realizados.

2.2.4 Segurança em pessoas

Aborda o conjunto de controles com o objetivo de reduzir os riscos de erro humano, intencionais ou não, pelo estabelecimento de responsabilidades relativas à segurança na descrição dos cargos, na forma de contratação e no treinamento em assuntos de segurança.

2.2.5 Segurança ambiental e física

Este tópico aborda os controles para prevenir acesso não autorizado, danos e interferências às informações e instalações físicas da organização.

2.2.6 Gerenciamento das operações e comunicação

Aborda as questões relativas a procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações e pelas respostas a incidentes. Envolvem questões como mudanças operacionais, gerenciamento de incidentes, definição de ambientes de desenvolvimento e produção, planejamento da capacidade, procedimento de cópias de segurança e prevenção e combate a vírus, entre outros.

2.2.7 Controle de acesso

Tem como objetivo controlar o acesso à informação baseado nos requisitos de segurança e de negócio. Procedimentos devem ser estabelecidos para o gerenciamento de privilégios, direitos e senhas de acesso aos sistemas e informações. Também devem ser estabelecidas regras para desconexão de terminais por inatividade ou por tempo de uso e para monitoração desses acessos, sejam locais ou remotos.

2.2.8 *Desenvolvimento e manutenção de sistemas*

Trata dos controles para garantir que a segurança seja parte integrante dos sistemas de informação. Isto inclui infraestrutura, aplicações do negócio e aplicações desenvolvidas pelo usuário. Deverão ser identificados e acordados os requisitos de segurança antes do desenvolvimento dos sistemas.

2.2.9 *Gestão da continuidade do negócio*

Trata dos controles parra evitar ou minimizar interrupções nas atividades do negócio e proteger os processo críticos contra conseqüências de falhas ou desastres significativos. Para tanto, deverão ser definidos planos de continuidade e contingência que deverão ser documentados, testados e atualizados.

2.2.10 *Conformidade*

Este tópico aborda os controles para evitar a violação de qualquer legislação, direitos ou obrigação, tais como propriedade intelectual e informações protegidas de clientes.

Cuidado especial deverá ser dado na definição da *política de segurança*, pois para os usuários é ela quem ditará as regras de utilização dos recursos e influenciará, inclusive no nível comportamental dos mesmos. A política serve a vários propósitos. Inicialmente, ela estabelece o que é e o que não é permitido. Ela deve estar alinhada com os objetivos de negócio da empresa. Ela serve para proteger também o próprio negócio [Maiwald e Sieglein, 2002], definindo como os empregados podem usar os recursos, estabelecendo, por exemplo, que só podem ser usados para a condução dos negócios da companhia, evitando assim problemas trabalhistas quando da demissão de um empregado que tenha desenvolvido um pequeno negócio próprio no computador da empresa. Segundo ainda Maiwald e Sieglein, uma política deve ser genérica o suficiente para que não haja a necessidade de mudanças freqüentes e, ao mesmo tempo, específica para evitar ambigüidades e possibilidades de interpretações, o que pode ser obtido através de procedimentos que complementem a política. Ela deve ser entendida e aceita por todos os usuários.

No projeto de segurança de cada empresa, além dos tópicos considerados básicos pela norma e daqueles referentes à *Política de segurança* conforme citado anteriormente, devem ser selecionados aqueles que se adeqüem à legislação e regulamentações vigentes e aos processos de negócio da corporação, ou seja, aqueles que contribuam para minimizar riscos considerados inaceitáveis para o sucesso do negócio.

No presente trabalho, podemos citar que terão mais peso aqueles relacionados à *Segurança física* que faz referência à prevenção de acesso não autorizado, dano e interferência às informações e instalações físicas da organização, ao *Gerenciamento das operações e comunicação* que se preocupa por exemplo com a questão dos vírus e cópias de segurança, ao *Controle de acesso* que envolve, principalmente, o acesso seguro (autenticação forte) e apropriado (perfil de direitos) à informação tanto a partir do próprio ambiente interno quanto do mundo externo à corporação.

2.3 Problemas de Segurança

Os inúmeros problemas que o mundo empresarial hoje vivencia através do ambiente tecnológico que deve proteger a informação podem ser ilustrados pelo resultado d uma pesquisa nacional da Symantec [Symantec, 2002], uma das grandes empresas mundiais em tecnologia de segurança de Internet, feita com base nas respostas de 240 executivos a um questionário com o objetivo de desenhar um cenário sobre a segurança de sistemas nas empresas do país.

De acordo com os resultados, 67% das companhias representadas pelos profissionais já sofreram algum tipo de ataque à rede, sendo que a origem foi vírus em 74% dos casos, abuso do uso de Internet por funcionários (73%) ou invasão externa do sistema (38%). Em 25% das ocasiões, os problemas foram causados por falta de conhecimento e treinamento de funcionários e em 16% por acesso não autorizado de internos à empresa (quebra ou uso indevido de senhas).

Um dado curioso é que 38% dos executivos afirmaram que os ataques foram de origem externa (hackers), 7% de procedência interna (funcionários) e 48% de ambas as formas - um porcentual de 86% de invasões. Vale ressaltar que, apesar do baixo

percentual de ataques de procedência interna, normalmente são esses que provocam os maiores prejuízos às empresas.

Seis em cada dez executivos disseram que suas empresas possuem site para comércio eletrônico e quatro entre dez que a página já fora atacada. Na maioria das ocasiões, o que ocorreu foi vandalismo (64%) e quebra de serviço, ou denial of service (25%). A incidência teve origem externa em 84% dos episódios. Os prejuízos ocorridos foram em sua maioria (76%) relacionados à impossibilidade de manter a empresa em operação.

Como se pode observar, das formas mais variadas, as empresas convivem diariamente com infinidades de tipos de problemas que podem ser agrupados basicamente na relação a seguir descrita.

2.3.1 Senhas

A utilização de senhas é parte especifica da segurança de informação e pelo fato de serem simples de usar, familiares e não requerer hardware especial, são utilizadas pela grande maioria dos sistemas de autenticação mas são consideradas um meio de proteção ineficiente, principalmente porque dependem do "elo mais fraco da corrente de segurança" que é o usuário.

As senhas, além de serem um fator importante em um sistema de segurança, também o são quanto à produtividade dos usuários. Na maior parte das empresas existe um grande numero de sistemas onde é necessário que se autentique em cada um deles, fazendo desta forma com que o usuário tenha que administrar varias senhas. Essa diversidade de senhas geralmente leva a uma de duas situações: numa, o usuário deixará anotadas as várias senhas e, na outra, provavelmente, definirá senhas iguais usando normalmente uma senha fraca; em qualquer das situações tem-se a segurança comprometida.

O esquecimento da senha é um fato comum e tem como conseqüência a diminuição da produtividade do usuário e o aumento dos custos com centrais de atendimento. Segundo um estudo do Hurwitz Group, uma empresa americana de consultoria,

pesquisa e análise de negócios em tecnologia, 61% das ligações telefônicas atendidas pelas centrais é devido ao esquecimento de senhas.

Senhas são ineficientes e passíveis de ataques. O ser humano consegue memorizar apenas senha sem muitos caracteres, o que compromete sua eficiência, em comparação com uma senha aleatória. Por outro lado uma senha aleatória é difícil de ser memorizada pelo usuário, e isso também pode causar problemas, pois geralmente, nesse caso, é preciso anotar a senha em um pedaço de papel, por exemplo. Assim, a conscientização dos usuários quanto aos perigos de uma senha mal escolhida é fundamental [Nakamura e Geus, 2002].

O comportamento dos usuários na escolha das senhas pode ser observado por meio de uma pesquisa realizada pela COMPAQ, em 1997, onde foi observado que as senhas são escolhidas da seguinte maneira:

Posições sexuais ou nomes alusivos a chefes (82%).

Nomes ou apelidos de parceiros (16%).

Nome do local de férias preferido (15%).

Nome do time ou jogador (13%).

O que se vê primeiramente na mesa (8%).

2.3.2 Internet

A Internet esta cada vez mais sendo utilizada por empresas e Governos para distribuir informações importantes e conduzir transações comerciais e financeiras. Junto com os aspectos positivos tais como a agilização das comunicações entre pessoas e empresas e o ganho de produtividade, trouxe também uma série de problemas decorrentes tanto de falhas tecnológicas quanto de ações criminosas.

Correio Eletrônico

Estatística da Wordtalk Corp, um instituto de pesquisa americano, mostra que de todos os e-mails 32% tem conteúdo inadequado (paqueras, correntes, informações

sigilosas), 9% vêm com grandes arquivos anexados e 8% contém vírus, números não muitos diferentes do Brasil, onde mais de 50% das mensagens que trafegam nas redes corporativas são consideradas "lixo" segundo um diretor da GS Sistemas, empresa especializada em segurança. Esses números podem ser traduzidos em baixa produtividade dos empregados envolvidos, necessidade de maior largura de banda de trafego e mais discos para armazenamento de mensagens. Na CTEEP, no período de um mês, são contabilizados mais de 200.000 e-mails somente de/para Internet. Não estão incluídos, portanto, todo o trafego interno de mensagens.

No Boletim da IDGNow de 23/10/02 é citado um estudo recente da MessageLabs, empresa americana provedora de serviços gerenciados especializada em segurança de e-mail, em que foram analisadas 63 milhões de mensagens para detectar aquelas não solicitadas, as chamadas spam. Desse total, 17% (quase 11 milhões !!!) eram spam.

Navegação

Paradoxalmente, a Web, permitindo a navegação pelo "mundo" com a sua facilidade e a agilidade levando a ganhos de produtividade, é responsável, ao mesmo tempo, pelo desperdício de recursos, tanto tecnológicos quanto de força de trabalho de uma grande parte dos empregados da empresa. Para ilustrar a gravidade do problema de uso improdutivo da Internet, no caso de navegação, consideremos o exemplo hipotético de uma empresa com 1000 empregados com custo salarial médio de R$3.000, equivalentes a R$15/hora: se, na média, cada empregado passar uma hora por dia em navegação dissociada de sua atividade profissional, ao final de um ano, a empresa terá pago para essa "atividade" um montante de R$4.500.000 (R$15 x 25 dias x 12 meses x 1000 empregados).

Ataques

Empresas podem sofrer ataques que vão desde, por exemplo, a simples pichação de páginas corporativas até aqueles com conseqüências que põem em risco a sobrevivência de empresas. Conforme citado no artigo "Esquema de falsificação de informação: o desafio de proteger conteúdo" [Beal, 2002] , em sua edição de agosto de 2002, a Revista Computer, da IEEE, tratou do tema "Cognitive Hacking", um tipo

de ataque à segurança da informação que se vale da manipulação de informações para alterar o comportamento de usuários a partir de dados falsos ou sutilmente alterados. A revista cita o exemplo de uma empresa que em 2000 foi atacada com a divulgação da notícia de que estava revendo o ganho por ação de US$.25, previamente anunciado, para uma perda de US$.15. Em 16 minutos, as ações daquela empresa despencaram de US$104 para US$43, antes que se descobrisse que o press release que anunciava o prejuízo, divulgado por diversas agências de notícias, havia sido falsificado por um hacker de 23 anos, com o propósito de obter lucro no mercado de ações.

2.3.3 Vírus

Com a Internet, a distância entre dois pontos distantes como o Japão e o Brasil, pode ser percorrida em questão de minutos, ou mesmo até segundos, o mundo se reduziu a uma pequena tribo, onde interagimos abertamente ou no anonimato. Com muita facilidade e em pouco tempo recebemos, enviamos e acessamos informações, tudo muito perto e disponível, foi quebrada a barreira da distância. Uma rede assim tão poderosa não deixa de esconder dentro de si imensos perigos em potencial.

A tecnologia da informação não trouxe apenas novas possibilidades de negócios para as empresas, trouxe também os vírus. Juntamente com as perspectivas excelentes do comércio eletrônico e business-to-business (B2B), figuras menos excitantes mas bastante poderosas invadem as nossas máquinas.

Além da interpretação de senhas e tráfego de informações, invasões a redes e quebra de privacidade, o mar de informações disponíveis pela Internet também expõe o navegador a arquivos infectados e códigos maliciosos.

Nem todos os vírus desenvolvidos no mundo chegam a destruir e ganhar importância. Mesmo assim, estima-se que a cada dia surgem de 10 a 20 novos vírus que causam algum tipo de estrago. Apenas no ano de 99 o mundo teve uma perda de 12,1 bilhões de dólares, segundo dados da empresa Computer Economics, por causa desses programas hostis.

Essa ameaça vem crescendo na mesma proporção em que a Web também se expande no espaço cibernético. A International Computer Security Association, sumidade internacional neste tema, constatou em uma pesquisa que o número de ataques nos meses de janeiro e fevereiro de 1999 representa o dobro das ocorrências de todo o ano de 1998 e quatro vezes maior que o total de investidas de 1997.

Infelizmente não basta comprar um "programa de antivírus" para estarmos livre de problemas. Uma proteção segura, implica em uma política complexa e rigorosa, que inclui desde a cobertura de qualquer porta de entrada de vírus, a definição de regras de uso dos recursos, o estabelecimento de uma rotina periódica de atualização das vacinas e, o mais importante, a colaboração do usuário final. Sem isso é impossível combater os mais fortes inimigos que surgem diariamente e que hoje não demoram mais do que 48 horas para fazer os maiores estragos pelo mundo afora.

Nenhuma empresa está 100% segura, pois as vacinas são criadas somente depois que um novo vírus é descoberto, mas os laboratórios dos fabricantes de programas de antivírus têm sido rápidos.

2.3.4 Segurança física

Uma lista das ameaças à segurança física poderia conter os seguintes itens:

- Incêndio (fogo e fumaça);
- Água (vazamentos, corrosão, enchentes);
- Tremores e abalos sísmicos;
- Tempestades, furacões;
- Terrorismo;
- Sabotagem e vandalismo;
- Explosões;
- Roubos, furtos;

- Desmoronamento de construções;
- Materiais tóxicos;
- Interrupção de energia (bombas de pressão, ar-condicionado, elevadores);
- Interrupção de comunicação (links, voz, dados);
- Falhas em equipamentos;
- Falta de controle no acesso às instalações;
- Outros.

O episódio de 11 de Setembro do World Trade Center teve como uma das conseqüências um alerta para as empresas investirem num bom projeto de segurança física; logicamente, a probabilidade de ocorrência daqueles fatos era quase nula, mas serviu de exemplo para aqueles que adotam, ou deixam de adotar, planos de segurança baseados na crença de que aquilo jamais vai acontecer com eles. São citados alguns casos de empresas que, mesmo tendo o sistema numa das torres e mantinham a contingência (site back-up) na outra, acabaram perdendo as informações.

Outro caso, este inclusive ocorrido bem próximo dos autores, foi o incêndio num dos prédios da antiga Cesp.

Casos que tem aumentado e que tem sido citados em artigos de segurança é o roubo de notebooks de empregados, normalmente executivos, em trânsito; nestes casos, o mais grave, além da perda do equipamento, é a perda de informações críticas ou estratégicas da empresa.

Casos bastante comuns são o roubo de equipamentos e de componentes, tais como pentes de memória, discos rígidos e outros periféricos; nestes casos, também o agravante é a perda de informações críticas armazenadas nos discos.

2.3.5 Roubo de Informação

Uma das ocorrências que mais prejuízo provoca no negócio de uma empresa é o roubo de informações críticas e estratégicas.

Com as inúmeras possibilidades de acesso ao mundo externo e de gravação de informações em diversas mídias de alta capacidade de gravação, aumentou-se significativamente o risco daquele problema. A liberação e instalação de placas fax/modem e de gravadores de CD/DVD permitem que se envie, seja pela transmissão eletrônica ou pelo transporte das mídias, informações críticas, na maioria das vezes sem nenhum controle.

No caso das placas fax/modem, o acesso ao mundo externo é feito desviando-se dos mecanismos de proteção e monitoramento normalmente instalados nas médias e grandes empresas, mecanismos estes implementados pelos firewall, proxy e os vários filtros das diversas ferramentas de mercado que estão apresentadas no capítulo 3 deste trabalho.

A proliferação de gravadores de CD propiciada pelo baixo custo e facilidade de uso permite que se crie condições de vazamento de informações, seja para uso pessoal ou para concorrentes do negócio.

Considerando uma das conclusões de pesquisa já citada anteriormente, a de que os autores dos maiores danos são os usuários internos, essas facilidades devem ser liberadas com bastante critério explicitado pelas regras e diretrizes de uma política de segurança bem definida.

3 SOLUÇÕES TECNOLÓGICAS

Apesar das dificuldades para se garantir a segurança da informação decorrente das falhas e vulnerabilidades do ambiente de Tecnologia da Informação como um todo, a implementação coordenada de políticas, procedimentos e práticas de segurança e de ferramentas tecnológicas, objeto deste trabalho, minimiza não só o número de incidentes como as suas conseqüências.

Como na vida real, não existe segurança total no mundo virtual. Na prática, como os recursos para investimentos são limitados, pessoas e organizações assumem riscos calculados através da análise do custo das soluções e do valor da informação, tangível ou não, a ser protegida. Após a consideração desses riscos selecionam-se ferramentas que, inseridas numa arquitetura bem planejada, mais se adeqüem àquilo que se vai proteger.

Algumas dessas principais ferramentas são apresentadas nesse capítulo:

Criptografia - É a técnica que, aplicando algoritmos matemáticos, codifica uma informação, dados ou mensagens, com o objetivo básico de garantir o seu sigilo. Usada desde os tempos antigos na forma mais primitiva conhecida como simétrica, o seu uso foi sendo aperfeiçoado com a adoção de novas técnicas e suas variantes. Como produto da criptografia, utilizam-se atualmente os chamados certificados e assinaturas digitais que permitem a troca de informações e a prática de comércio eletrônico de forma segura; para facilitar o uso e garantir legalidade dessas transações eletrônicas, há necessidade de regras, padrões e procedimentos que, no caso do Brasil, foram implementados pela chamada infra-estrutura de chaves públicas, a ICP-Brasil.

VPN (Virtual Private Network) - As redes públicas, base de comunicação da Internet, são consideradas inseguras. Entretanto, têm custo significativamente mais baixo se comparadas com as redes proprietárias. Transformando um meio inseguro em um meio confiável, a VPN permite o uso das redes públicas garantindo o sigilo das comunicações através da implementação de recursos e técnicas de segurança.

Antivírus - Com a freqüência com que têm surgidos novos vírus, é imprescindível não só dispor de programas antivírus como tê-los com recursos e facilidades que garantam a proteção de forma ágil e transparente. Os atuais programas antivírus implementam recursos que, minimizando a necessidade de intervenção "manual", automatizam várias tarefas e otimizam o uso dos recursos do ambiente.

Firewall - É um componente de segurança baseado em hardware e software com o objetivo de proteger computador ou rede de computadores. Como uma parede de fogo, da tradução literal, instalado no limite da rede pública e a rede corporativa, funciona como uma proteção contra os vários tipos de ataque que podem ocorrer, principalmente no mundo Internet. Basicamente, implementam três formas de proteção: seleção ou filtragem dos vários tipos de pacotes do protocolo TCP/IP, mascaramento dos endereços IP e o proxy que, como um procurador, executa de forma eficiente as tarefas solicitadas por pessoas devidamente autorizadas ou autenticadas.

IDS (Intrusion Detection System) - O IDS, como o firewall, tem como função a proteção de computador ou rede de computadores contra tentativas de invasão; entretanto, diferentemente daquele, o IDS analisa e alerta "comportamentos" do invasor tais como ataque automatizado de senha ou varredura de portas à procura de serviços que, mesmo não sendo utilizados, são mantidos ativos como configuração padrão e sujeitos a falhas e vulnerabilidades que facilitarão a invasão.

Backup - É o item de segurança mais difundido e usado nos ambientes corporativos. Tão importante quanto às ferramentas de cópia e restauração são os procedimentos que definem, por exemplo, a periodicidade de execução das cópias de acordo com o que se deseja proteger e as responsabilidades pelas ações a serem tomadas e, também, os tipos de mídia a serem usados considerando a necessidade de regravações e o tempo que a informação necessita ser mantida.

3.1 Criptografia

CRIPTOGRAFIA (de kryptós = escondido,oculto + grápho = grafia) , conforme a definição do dicionário Michaelis, "é a arte ou processo de escrever em caracteres secretos ou em cifras".

A criptografia é usada desde os tempos de Júlio Cesar que, não confiando nos mensageiros, enviava mensagens aos seus generais utilizando-se da forma mais primitiva de codificação, deslocando um determinado número de posições as letras do alfabeto, trocando por exemplo a letra A pela D, a B pela E e assim sucessivamente. Nesta técnica, adotando-se o deslocamento de 3 letras, a palavra "segredo" era transformada em "vhjuhgr" e era compreendida somente pelo destinatário que conhecia a "chave" ou o "segredo" do esquema, no caso "deslocar 3 letras". Apesar de simples, este exemplo ilustra didaticamente o funcionamento básico da criptografia [NAI, 1.999].

Como citado, já naquela época havia a preocupação com a confidencialidade das informações.

No mundo "internetizado" de hoje, com a troca constante de informações seja através de arquivos ou de correio eletrônico por meios nem sempre seguros como a Internet que se utiliza da rede pública de comunicação, tornou-se imprescindível a adoção de técnicas que garantam o quesito do sigilo. Para tanto, a criptografia atual utiliza-se de sofisticados algoritmos matemáticos que tem como objetivo básico a transformação da informação, arquivo ou texto, em informação cifrada que ao chegar ao seu destinatário é revertida para o original pela mesma sistemática.

O poder do sistema criptográfico utilizado pode ser medido em função do tempo e recursos necessários para a descoberta do "segredo". Considerando a capacidade dos processadores atuais e, principalmente, a possibilidade de processamento cooperativo de máquinas ligadas pelas velozes redes, os sistemas criptográficos atuais podem ter seu "segredo" quebrado, tratando-se apenas questão de tempo. Existem publicações de pesquisas teóricas que mostram que máquinas construídas especificamente para esse fim conseguem, em questão de dias e até horas dependendo dos recursos

investidos (basicamente, número de processadores trabalhando de forma coordenada), descobrir a chave utilizada através do método da "força bruta", isto é, tentando todas as combinações possíveis que o tamanho da chave escolhida permite. Como exemplo do cuidado e da importância dedicados ao assunto, pode ser citado o DES, Data Encryption Standard, o tradicional método de criptografia que utiliza uma única chave para cifrar e decifrar e por isso considerado simétrico, apesar de permitir a escolha do "segredo" dentre as 72.000.000.000.000.000 (2^{56}) combinações possíveis pode ser quebrado em questão de horas. Outro exemplo que pode ser citado é o caso dos desafios lançados pelos laboratórios da RSA Security, uma das mais renomadas empresas em segurança eletrônica, que premia pessoas ou equipes que desvendam as chaves dos diversos algoritmos e que tem como objetivo verificar o poder dos algoritmos e confirmar as estimativas teóricas que vão auxiliar a indústria a investir na melhoria contínua das soluções de segurança; conforme um boletim [RSA, 2002] daquela empresa, uma equipe de 331.252 voluntários, entre cientistas, programadores e usuários conhecida como "Distributed.Net", solucionou, após quatro anos, o desafio da chave secreta do algoritmo RC5-64 utilizando os momentos ociosos dos seus computadores distribuídos por todo o mundo que procuraram todas as possibilidades da chave de 64 bits do RC5.

Na teoria, não existe algoritmo que não possa ter a chave utilizada descoberta. Entretanto, apesar dessa aparente fragilidade deve ser considerado o lado prático e para tanto a escolha dos algoritmos a serem usados tem que levar em consideração o "valor" da informação a ser protegida e o tempo de duração dessa proteção. Quanto maior forem esses parâmetros maior o cuidado na escolha do mecanismo de criptografia.

A seguir são apresentados alguns conceitos e as principais técnicas dos criptosistemas.

A princípio, a criptografia pode ser classificada em dois grandes grupos: a de chave simétrica ou convencional e a assimétrica ou de chave pública.

Na criptografia de chave simétrica ou convencional uma única chave é usada tanto para cifrar quanto para decifrar. A figura 4 a seguir ilustra o processo.

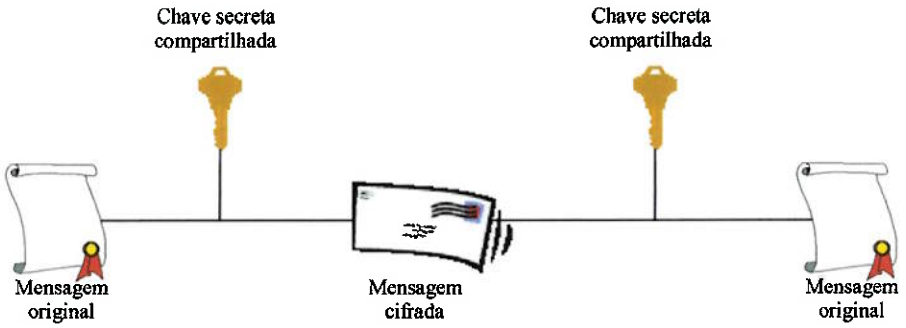

Figura 4 - Processo da criptografia simétrica

O exemplo atual mais conhecido é o DES anteriormente citado. Nesse algoritmo, cada bloco de 64 bits de informação, texto ou dado, é encriptado com uma chave de 56 bits. Para aumentar a confiabilidade do sistema implementam-se melhorias na criptografia simétrica. O método mais conhecido é o de aplicar vários passos do sistema original; aplica-se inicialmente o algoritmo com uma chave de 56 bits, decifra-se o texto cifrado com uma chave diferente da primeira e, finalmente e novamente, encripta-se com a chave original, aumentando-se a efetividade da chave de 56 bits para 112 bits. O 3DES é uma implementação dessa técnica, com a diferença que utiliza três chaves distintas no processo, o que aumenta ainda mais a segurança, pois tem-se agora uma equivalente chave de 168 bits.

Em geral, a execução dos sistemas de chave simétrica é rápida, ideal, portanto, para a transferência segura de grandes volumes de informação. A mesma chave usada para cifrar deverá ser informada ao destinatário da mensagem para que o mesmo possa decifrá-la. Numa situação bastante comum, enviar mensagem para várias pessoas localizadas em vários locais revela a grande desvantagem desse sistema: transmitir, de forma segura e com custo baixo (telefone, fax, mensageiro ?) a chave secreta para os diversos destinatários; uma nova mensagem para um outro grupo implica em uma nova chave e um novo esquema de distribuição.

O segundo grupo de sistema criptográfico é o de chave assimétrica ou de chave pública, conceito introduzido por Whitfield Diffie e Martin Hellman em 1975. Nesse sistema usa-se um par de chaves, a pública e a privada. A primeira como o próprio nome sugere é de conhecimento de todos os interessados, enquanto que a segunda é

proprietária e de conhecimento somente do seu dono. A criptografia é feita com a chave pública do destinatário e o processo de reversão é possível somente com a correspondente chave privada. Como a relação das chaves pública e privada é biunívoca , somente o destinatário conseguirá decifrar a mensagem. Na figura 5 a seguir é mostrado o esquema do sistema de encriptação através de chave pública.

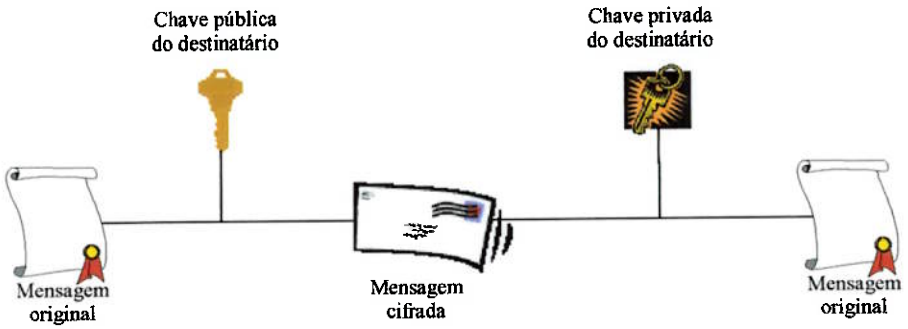

Figura 5 - Esquema da criptografia de chave assimétrica

A dificuldade relacionada com segurança e custo de distribuição das chaves do sistema simétrico é eliminada no caso de chave pública. Nesse, a entidade, pessoa física ou jurídica, divulga a sua chave pública para qualquer interessado na troca de informações.

Além de garantir a confidencialidade e integridade da mensagem e da facilidade de distribuição das chaves, o sistema de chaves públicas, uma revolução em criptosistemas, permite o seu uso para garantir a autenticidade e o "não repúdio", outros quesitos da segurança da informação. Com ela implementa-se a chamada assinatura digital que permite que o destinatário da mensagem se assegure sobre a identidade da pessoa que enviou e, conseqüentemente, evite a negação ou o "repúdio" daquele ato. Esses quesitos são hoje imprescindíveis para a viabilização de transações de comércio eletrônico, transações financeiras, etc... Para se conseguir isso, além de cifrar a mensagem com a chave pública do destinatário, o remetente usa também a sua chave privada; no processo executado no destino, o uso da chave privada do destinatário garante a privacidade e a confidencialidade da mensagem e a chave pública do remetente garante a sua identidade.

O sistema de chave pública mais conhecido é o RSA, nome originado dos seus autores Ron Rivest, Adi Shamir e Leonard Adlemn. Esse método baseia-se em teoria dos números primos que mostra a dificuldade de se fatorar o produto obtido pela multiplicação de dois números primos grandes.

A desvantagem dos sistemas assimétricos é o tempo de execução do seu algoritmo. O PGP, Preety Good Privacy, combina características dos sistemas simétricos e assimétricos, por isso chamado criptosistema híbrido ou misto. No PGP, o texto é cifrado pelo método convencional, portanto rápido, com uma chave de sessão válida somente uma única vez e que é gerada randomicamente com parâmetros como movimentos do mouse e teclas digitadas; a chave é, então, encriptada com a chave pública do destinatário e encaminhada junto com o texto cifrado. A figura 6 mostra o esquema do PGP.

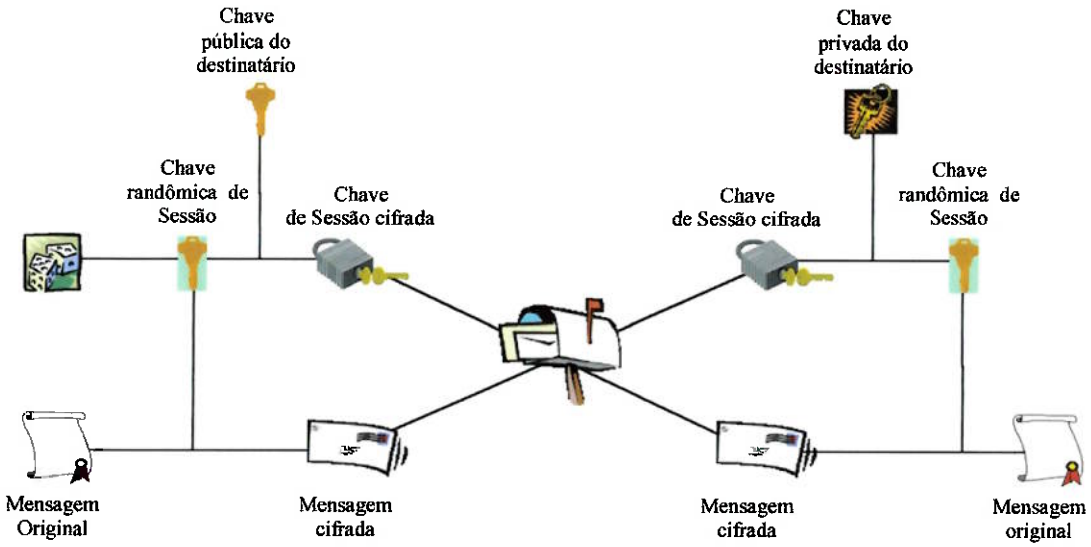

Figura 6 - Esquema do criptosistema PGP

Portanto, os sistemas mistos têm como característica a velocidade do método convencional, através da chave de sessão, e a conveniência do método da chave pública que elimina o problema da distribuição de chave garantindo o sigilo do "segredo" e, como conseqüência, obtém performance com segurança.

A tabela mostra um resumo comparativo dos métodos de criptografia simétrica e assimétrica:

Comparativo Simétrico X Assimétrico

	Simétrico	**Assimétrico**
Velocidade	Rápido	Lento
Tamanho da chave	Relativamente pequena	Extremamente grande
Uso da chave	Segredo compartilhado	Pública/privada
Aplicação	Grande volume de dados	Autenticação
Exemplo + conhecido	DES, 3DES	RSA, PGP

3.1.1 Assinatura e Certificado Digital

Outra implementação decorrente da criptografia atual é a dos certificados digitais que tem como principal função garantir a identidade de quem diz ser. No mundo inseguro da Internet que se utiliza das redes públicas de comunicação passíveis de serem interceptadas ou dos servidores que sem a implementação de um mínimo de segurança podem ser invadidos ou "clonados", é vital garantir a identidade de quem diz ser.

Um certificado digital é um "documento" eletrônico que tem a função básica de comprovar a identidade da pessoa que está acessando algum serviço que tenha essa exigência de identificação segura ou de máquinas servidoras que têm que ter a sua identidade assegurada perante os seus usuários, tais como parceiros trocando informações críticas do negócio ou de compradores de produtos através do comércio eletrônico ou de usuários de serviços prestados por entidades financeiras.

Como já citado, a chave pública de um destinatário garante a segurança do segredo da mensagem; entretanto, quem garante que a chave realmente pertence ao parceiro com quem achamos que estamos trocando informações ? A resposta está no certificado digital que vincula uma chave pública de uma pessoa ou organização.

Certificados digitais como por exemplo o documento "Registro Geral - RG" contém informações para a sua identificação e devem ser emitidos, após confirmados os dados fornecidos pelo solicitante, por uma entidade confiável, tal como ocorre naqueles que são emitidos pelas Secretarias de Segurança Pública (SSP) de Estado. São emitidos por uma entidade denominada Autoridade Certificadora CA (Certificate Authority), que pode ser a própria organização cujos parceiros confiam nos seus certificados ou uma terceira entidade juridicamente estabelecida que, como no caso das SSP, antes da emissão tomam as providências para garantir a idoneidade do solicitante.

Um certificado digital contém, entre outras informações, uma identificação ou número de série única, o nome da CA emissora, o período de validade, alguns dados do algoritmo usado e um código digital equivalente à "impressão digital" ou assinatura digital da CA que atesta a autenticidade do certificado através de uma entidade confiável.

3.1.2 PKI / ICP-Brasil

PKI, do inglês Public Key Infrastructure, é um conjunto de técnicas, tecnologias, prática e procedimentos implementados para viabilizar no mundo real o uso dos conceitos que garantem o sigilo da informação e a sua autenticidade como aplicação prática da teoria vista no decorrer deste capítulo.

A PKI permite e facilita a efetivação de transações eletrônicas entre os participantes do mundo Web, Internet, Intranet ou Extranet. Organizações ou pessoas, mesmo que não se conheçam ou estejam geograficamente distantes, podem manter relacionamentos baseados na confiança através de terceiros, elemento chave da PKI, as chamadas autoridades certificadoras: A confia em B, C confia em B, portanto, A confia em C.

A infra-estrutura necessária pode ser implementada pela própria organização que tem que se relacionar com seus empregados e parceiros. Ela própria executa os serviços que facilitam esse relacionamento de confiança, mas à medida que esse relacionamento vai crescendo vai aumentando a dificuldade para o seu

gerenciamento e manutenção; como conseqüência surge a necessidade de entidades especializadas que prestem esse tipo de serviço, surgindo, então, as autoridades certificadoras.

Na parte de serviços uma PKI disciplina e define padrões e regras de modo a facilitar o seu acesso e uso pelas organizações ou pessoas que podem solicitar, entre outros:

- emissão de um novo certificado;
- revogação ou cancelamento de certificados;
- publicação das chaves públicas dos usuários;
- validação de um certificado;
- verificação de operações autorizadas no certificado;
- recuperação das chaves de um usuário.

O Governo Brasileiro, por meio da edição da Medida Provisória MP n.º 2.200, de 28 de junho de 2001, instituiu os meios e regras técnicas pelos quais possibilita a habilitação de instituições públicas e organismos privados a atuarem na validação jurídica de documentos produzidos, transmitidos ou obtidos sob a forma eletrônica.

Conforme a definição no site www.icpbrasil.gov.br, a Infra-estrutura de Chaves Públicas - ICP Brasil "é um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública".

Os meios e regras técnicas da MP 2200 destinam-se, conforme texto da MP, a "garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".

Com essa medida passou-se a dispor de alternativa para realizar eletronicamente transações que até agora não se podiam fazer e exigiam registros em papel escrito

para adquirirem validade. Essa nova modalidade de documentos não exclui nem se sobrepõe aos documentos utilizados atualmente. São equivalentes e isonômicos. Isto é, o sistema de certificação eletrônica não introduz conceitos novos nas transações, apenas estabelece equivalência e isonomia legal entre os documentos produzidos e obtidos eletronicamente e os documentos firmados em papel, desde que certificados na IPC - Brasil. Isso significa que as certificações realizadas por entidades certificadoras não vinculadas à ICP-Brasil poderão continuar sendo feitas. Nessa condição, ao certificar determinado documento, as entidades o atestam quanto à sua autenticidade e integridade, de modo semelhante a uma testemunha.

Já no caso de uma entidade certificadora vinculada ao sistema IPC-Brasil, seus documentos gozarão de uma presunção de autenticidade derivada da lei. É importante lembrar que as operações e transações feitas com ou sem certificação, efetuada por entidades certificadoras não vinculadas, mantém a validade relativa que lhes é garantida nos respectivos contratos e nas leis civis e comerciais do país e continuarão a tê-la.

Até o momento, já estão credenciadas algumas autoridades certificadoras: Serpro, Serasa, Certsign, SRF (Secretaria da Receita Federal) e Caixa (Econômica Federal) e que são licenciadas pela denominada autoridade certificadora raiz, a executora das políticas estabelecidas pelo Comitê Gestor ICP-Brasil.

3.2 VPN - Virtual Private Network

Nos tempos dos chamados mainframes as redes de teleprocessamento se restringiam a uma malha de terminais sem capacidade de processamento que eram interligados por meios de comunicação proprietários, conforme mostrado na figura 1. Com a proliferação de redes locais, as chamadas Lan, aumentou-se a complexidade conforme a figura 2 e os custos de se manter aqueles canais proprietários de comunicação. As redes agora são interconectadas através das várias opções disponíveis, especialmente aquelas oferecidas pelos prestadores de serviços público, meios utilizados e que contribuíram para o sucesso da Internet; as soluções atuais vão desde a mais simples chamada ponto a ponto que as ligam por uma linha telefônica pública, discada ou dedicada, e que tem como aplicação mais popular o acesso aos

serviços através do recurso "dial-up" do Windows e das conhecidas placas fax-modem até as mais sofisticadas tal como ATM de alta velocidade usando como meio de transferência satélites de comunicação e fibras óticas entre outros.

Atualmente no Brasil, após um crescimento explosivo de uso do frame-relay, está aumentando a procura por solução de conexão de redes corporativas através das chamadas VPN sobre IP que oferecem algumas vantagens em relação à implementação sobre outras tecnologias como ATM por permitir mais flexibilidade e facilidade de conexão, considerando, principalmente, que as redes corporativas já implementam serviços baseados no protocolo IP e Intranets através da tecnologia Web.

3.2.1 O que é VPN - Virtual Private Network

Por definição, VPN é um sistema que permite que duas ou mais redes privadas sejam conectadas através de infra-estrutura de comunicação pública como a Internet; assim, uma organização com suas várias filiais, independente da distância geográfica, pode, virtualmente, montar a sua rede corporativa utilizando-se da infra-estrutura pública tal como uma Wan, sem a necessidade de grandes investimentos.

3.2.2 Princípios da VPN

Utilizando-se do meio inseguro da Internet, é necessário que a VPN tenha implementadas algumas soluções de segurança. Deve garantir que a informação em trânsito não seja interceptada e que, caso isso ocorra, ela não possa ser reconhecida ou alterada até a chegada ao seu destino final. Isto é assegurado pela técnica de tunelamento, criptografia conforme visto no item 3.1, autenticação, tecnologias e serviços de controle de acesso.

O IP Security, mais conhecido como IPSec, é um conjunto de protocolos ou uma extensão do IP desenvolvido pela Internet Engineering Task Force, que implementa autenticação forte de dados e garantia de privacidade de modo que viabiliza a transferência segura de informações críticas através da criação de "túneis" entre os equipamentos de conectividade. Outro protocolo de tunelamento que implementa

essas soluções de segurança é o L2TP, uma combinação dos protocolos L2F, Layer 2 Forwarding, da Cisco e PPTP, Point to Point Tunneling Protocol, da Microsoft.

O complemento à segurança do tunelamento é feito com uma das técnicas de criptografia, escolha que deve considerar o nível de segurança exigido pelas informações a serem transmitidas conforme citado no item 3.1.

A implementação de uma VPN pode ser feita através de uma das três formas: baseada em hardware, em programas/softwares ou em firewall (vide item 3.4). A utilização de hardware como o roteador é o exemplo do primeiro caso que é considerado simples e seguro e, normalmente, é um equipamento já existente; tem a desvantagem de não ser muito flexível, requisito a ser considerado quando os pontos terminais não são controlados pela mesma empresa, situação típica do mundo globalizado relacionando vários parceiros de negócio. A implementação em firewall é considerada a mais segura, pois tem a vantagem de se aproveitar dos mecanismos de segurança já existentes naquela solução; nesse caso, importante consideração é a carga de trabalho da VPN que será adicionada ao firewall que já executa trabalho em atendimento às suas próprias funções.

3.2.3 Vantagens de uma VPN

A figura 7 abaixo mostra uma arquitetura de rede com solução VPN que permite a conexão de empregados, filiais e parceiros de negócio e que facilita a visualização das vantagens da solução VPN.

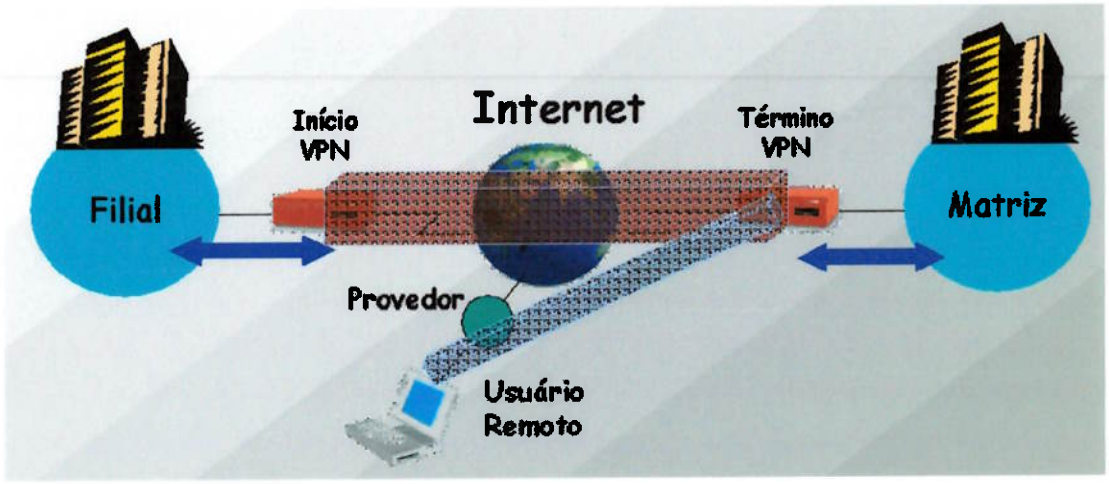

Figura 7 – Solução típica de uma VPN

Há um número de razões para se usar VPN, mas a mais significativa diz respeito ao seu baixo custo comparado ao de outras opções. Ao se usar a Internet para distribuir os serviços de rede sobre grandes distâncias, as empresas não mais necessitam manter caríssimos sistemas de comunicação proprietários e, nem mesmo, alugar caras linhas privadas de longo alcance para interligar as suas filiais ou seus parceiros. Numa empresa vivendo um forte crescimento ou numa multinacional com subsidiárias em vários países, esta vantagem faz grande diferença na escolha dessa solução.

Outra vantagem, também relacionada a custo, refere-se ao suporte e gerenciamento do sistema que, se fornecido pelo próprio provedor de serviços VPN, tem um custo menor em decorrência da diluição do custo total entre os seus vários clientes.

Normalmente as empresas mantém um sistema para acesso remoto de seus empregados, seja a partir de suas residências ou de empregados em trânsito. Para tanto, adotam solução RAS, Remote Access Server, que são implementadas por equipamentos, pool de modems e de linhas telefônicas, com um custo operacional alto. Com a VPN, elimina-se a necessidade desses recursos operacionais, com uma grande vantagem para o usuário, principalmente aquele que tem que fazer conexão dial-up de longa distância, que agora tem a opção de acessar a rede corporativa através de conexão ADSL em banda larga.

3.3 Antivírus

Segundo dados de pesquisa americana [CSI/FBI, 2002]realizada junto a 503 profissionais de segurança de organizações e entidades dos vários segmentos dos Estados Unidos, ano após ano os incidentes de ataques por códigos maliciosos, particularmente os vírus, têm sido citados como os de maior freqüência. São citados números absolutos de perdas que em 1997 totalizaram, para os que responderam a pesquisa, US$12,5 milhões com uma perda média por organização de US$75.000. Sempre crescente, em 2001, para os 186 que responderam a pesquisa, foram contabilizados mais de US$45 milhões com uma média de US$243.000 de prejuízo por empresa. Na última pesquisa, 2002, os quase US$50 milhões representaram uma média de US$283.000 por organização. Com a apresentação de mais alguns números

indicando gravidade equivalente a nível mundial, o capítulo referente a vírus dessa pesquisa é fechado com a colocação: "tire suas próprias conclusões".

Para o Brasil, analisando-se as várias edições das pesquisas realizadas pela Módulo Security [Módulo, 2002] também se verifica entre as primeiras colocações citadas as ocorrências de vírus.

O objetivo básico dos vírus digitais que atacam o mundo virtual é, praticamente, a mesma dos vírus reais: invadir e provocar destruição. No interior de uma célula viva, o vírus torna-se um organismo vivo que pode se multiplicar inúmeras vezes, causando o avanço da infecção na pessoa que o hospeda e que transmite para outra que apresenta um mínimo de predisposição para essa infecção [Leite, 2002]. A analogia é totalmente válida no mundo virtual: vírus são programas que se anexam a arquivos da máquina alvo, caracterizando a infecção; o arquivo hospedeiro, por sua vez, pode infectar outros num processo de replicação; assim se estabelece as condições para o alastramento dos vírus que pode ocorrer na transferência de arquivos através do intercâmbio de mídias e, principalmente, através da facilidade do correio eletrônico. Os vírus atuais se aproveitam das vulnerabilidades dos programas para invadir os sistemas e se "reproduzir"; o "nimda" que provocou recentemente grandes prejuízos se aproveitou de falhas conhecidas e divulgadas do navegador Microsoft Internet Explorer e do IIS, Internet Information Services, componente do Windows para aplicações Web.

Apesar do conceito extremamente simples, o combate a esse tipo de problema é, na prática, extrema e inversamente complexo.

A principal dificuldade para tanto está relacionada ao mau uso dos recursos disponíveis, particularmente o correio eletrônico que é o principal meio de propagação dos vírus, decorrentes de negligência ou ignorância.

Outra dificuldade está no fato de que o combate é sempre feito contra aquilo que se conhece. As boas ferramentas ou programas antivírus corretamente implementadas têm mecanismos de atualização automática de modo que garantem a proteção contra todas as pragas até então conhecidas. Mas o que ocorre quando de um novo vírus ?

Na agilidade dos fabricantes dos antivírus está a resposta, ou seja, há uma janela de tempo de insegurança na qual ocorrerão os seguintes passos: a detecção que pode ocorrer em qualquer lugar do mundo por qualquer pessoa ou entidade, a sua comunicação aos fabricantes de antivírus, a análise do código malicioso, o desenvolvimento da vacina e finalmente a sua divulgação. Dependendo dessa janela de tempo, poderá ocorrer o alastramento do vírus, caracterizando uma epidemia que, com o passar do tempo ou mais especificamente das horas, vai tornando cada vez mais difícil o seu combate, explicando, em parte, as grandes perdas financeiras citadas.

Atualmente as boas ferramentas de antivírus dispõem de mecanismos com o objetivo de utilizar de forma racional os recursos da infra-estrutura onde serão instalados e, também para garantir a sua operação correta e confiável, executar uma série de tarefas de forma transparente e automática, eliminando ou minimizando a necessidade de intervenção tanto da equipe de suporte e administração quanto do próprio usuário.

As principais facilidades estão relacionadas à atualização das chamadas "assinaturas", que são os "modelos" que contém as principais características identificadoras dos vírus, a partir das quais são feitas a análise e detecção. Essas assinaturas são criadas nos laboratórios de pesquisa dos fabricantes de antivírus tão logo alguma ocorrência de um novo vírus seja relatada em qualquer parte do mundo, quando então é estudado para a definição de suas características; uma vez testadas, elas são disponibilizadas para os clientes nos sites do fabricante. Disponível, ela deve ser obtida para atualizar o cadastro do sistema antivírus; esse procedimento de atualização deve ser executado de forma automática, não dependente da parte considerada a mais fraca do ambiente de segurança, ou seja, o usuário.

Num ambiente corporativo, com inúmeras estações de trabalho espalhadas por várias redes, próximas ou geograficamente distantes, é imprescindível que o sistema antivírus disponha de mecanismos que, além de facilitar a atualização conforme colocado anteriormente, permitam utilizar a infra-estrutura de comunicação e de serviços de forma eficiente, considerando todas as deficiências e restrições existentes tais como baixa velocidade de canais de comunicação entre redes, dificuldade de

alocação e deslocamento de equipes para a execução de tarefas como instalação, atualização e reparos, etc... Uma das características desejáveis a ser considerada é a possibilidade de integração com sistemas já disponíveis na rede local que permita, por exemplo, que tarefa como a instalação do antivírus numa nova estação de trabalho recém conectada à rede seja feita automaticamente quando do seu primeiro acesso a um serviço preexistente que, por sua vez, ativaria o procedimento para a execução da tarefa em questão.

Outro recurso interessante e importante para um ambiente corporativo é o gerenciamento das atividades do sistema. A ferramenta antivírus deverá atender a essa necessidade, permitir um controle centralizado, capturar informações das ocorrências em todo o ambiente, emitir relatório e estatísticas das ocorrências.

Numa típica configuração de ambiente antivírus, inicialmente, é instalado o sistema antivírus em um servidor de cada rede e num servidor central; operacionalmente, as principais atividades executadas, de forma automática, são relatadas a seguir:

- conexão de uma nova estação de trabalho na rede: no seu primeiro acesso a um serviço já disponível na rede, é disparado o processo de instalação automática do antivírus;

- detecção de um vírus na estação de trabalho: o sistema de detecção automática de vírus da estação detecta a presença de vírus em algum arquivo lido pela mesma, toma uma ação pré definida na configuração do sistema e comunica a ação tomada para o usuário e para o servidor correspondente;

- atualização da base de dados com a assinatura de um novo vírus: o servidor central ou primário, com uma freqüência pré-configurada, verifica no site do fabricante do sistema a existência de uma nova assinatura; na confirmação, faz uma cópia e a inclui em sua base de assinaturas; da mesma forma, os servidores de cada rede pesquisam constantemente a existência de novas assinaturas no servidor central;

- gerenciamento centralizado: toda ocorrência, tanto na estação de trabalho quanto nos servidores, é registrada no servidor correspondente; para que se tenha uma

visão global, a ferramenta de gerenciamento coleta os registros de ocorrência em todos os servidores da rede corporativa e, de forma consolidada, apresenta relatórios e estatísticas ao administrador que tomará as providências necessárias a cada situação apresentada.

3.4 Firewall

No início da era dos computadores, tudo que você necessitava para manter seguros os dados do seu computador eram uma senha e uma tranca na porta do seu escritório.

Daí vieram as redes de computadores, uma tecnologia que interliga computadores de forma que seus usuários podem compartilhar recursos e idéias. Isso alterou completamente a fórmula para garantir a segurança dos computadores.

De repente, travas e portas de escritório não mais protegiam os dados. Os potenciais invasores não necessitavam mais de acesso direto aos computadores para atacá-los. Eles podiam utilizar qualquer computador na rede, mesmo um do outro lado do mundo, para acessar qualquer outro computador.

O advento das redes de computadores também atraiu a atenção de um grupo de adolescentes bagunceiros que gostavam de utilizar equipamentos que fraudavam a companhia telefônica para fazer ligações de graça.

De dentro desse grupo vieram os hackers de computadores que gostavam ou obtinham lucros descobrindo senhas e invadindo qualquer rede de computadores que os atraísse, quer sejam rede privadas, confidenciais, vitais para empresas ou operações governamentais.

A maior parte do mundo prestou pouca atenção a essa ameaça, principalmente porque a vasta maioria das empresas e outras organizações não estavam ainda conectadas às redes de computadores. Na década de 80 a Internet ainda estava na sua infância, servindo principalmente universidade e instituições de pesquisas.

No entanto, poucas instituições de pesquisas, órgãos governamentais e corporações decidiram que eles deveriam proteger suas valiosas informações confidenciais contidas em seus computadores em rede. Entre elas estava o Bell Labs. Eles

construíram uma proteção para guardar uma rede de 1.300 computadores contra acessos não autorizados. Esses computadores estavam dentro da maior empresa de telecomunicações do mundo: a AT&T.

Os administradores de rede de todo o mundo entraram em pânico. Um novo mercado surgiu da noite para o dia para satisfazer a súbita demanda por segurança. Esse mercado começou a fornecer equipamentos de proteção de rede. Esse equipamentos ganharam o apelido de Firewalls

Os Firewalls são compostos por uma série de componentes, onde cada um deles tem uma funcionalidade diferente e desempenha um papel que influi diretamente no nível de segurança do sistema.

3.4.1 Componentes de um Firewall

Os Firewalls mantêm uma conexão à Internet a mais segura possível inspecionando e aprovando ou rejeitando cada tentativa de conexão feita entre a rede interna e redes externas, como a Internet. Firewalls poderosos protegem uma rede em todas as camadas de software, da camada de enlace dos dados até a camada de aplicação

Os Firewalls se localizam nas fronteiras da rede, nas interconexões (gateways) que fornecem acesso a outras redes. Por essa razão os Firewalls são considerados uma proteção das fronteiras. O conceito de proteção das fronteiras é importante - sem ele, qualquer host da rede teria de realizar as funções de um Firewall sozinho, consumindo inutilmente recursos de computação e aumentando o tempo necessário para conectar, autenticar e criptografar os dados nas redes locais de alta velocidade. Os Firewalls permitem centralizar todos os serviços de proteção em máquinas otimizadas e dedicadas a essa tarefa.

Por sua natureza os Firewalls criam passagens estreitas entre a rede interna e externa para que todo o tráfego entre uma e outra tenha de passar através de um único ponto de controle. Esse é um pequeno preço a se pagar pela segurança. Como as conexões de linhas diretas externas são relativamente lentas se comparadas com a velocidade dos computadores modernos, a latência causada pelos Firewalls pode ser considerada completamente transparente.

Os Firewalls operam usando primeiramente três métodos fundamentais:

Filtragem de pacotes - rejeita pacotes TCP/IP de hosts não autorizados e rejeita tentativas de conexão com serviços não autorizados.

NAT (Network Address Translation - conversão de endereços de rede) - Converte os endereços IP dos hosts internos para ocultá-los de qualquer monitoração externa. A NAT é também chamada de mascaramento de IP.

Serviços proxy - o servidor de proxy tem duas funções básicas: permitir a autenticação para a navegação e manter a tabela de cache atualizada para facilitar e agilizar as pesquisas na web.

Autenticação criptografada - Permite aos usuários da rede pública provarem sua identidade ao Firewall a fim de obter acesso à rede privada a partir dos pontos externos.

Túneis criptografados - Estabelece uma conexão segura entre duas redes privadas por meio de um meio público como a Internet. Isso permite que redes fisicamente separadas usem a Internet em vez de conexões de linhas diretas para comunicarem-se entre si. O tunelamento é também chamado de VPN (Virtual Private Networking, rede privada virtual).

Quase todos os Firewalls usam esses métodos básicos para oferecer um serviço de segurança.

Podemos usar dispositivos ou servidores que realizam somente uma das funções anteriores; por exemplo podemos ter um roteador que faça a filtragem de pacotes e depois um servidor proxy em uma máquina separada. Fazendo assim, o filtro de pacotes precisaria repassar o tráfego para o servidor proxy ou o servidor proxy precisaria ficar do lado de fora da rede sem a proteção da filtragem de pacotes. As duas formas são mais perigosas do que usar um único produto Firewall que realize todas as funções de segurança em um único lugar.

Basicamente, Firewalls são meios de regular o aceso à redes de computadores. Eles são muito parecidos com guardas que ficam nas recepções dos prédios de empresas.

Eles param as pessoas que entram no edifício, pedem identificação - os seus nomes, nome da pessoa no prédio sendo visitada e daí permitem a sua entrada se tudo estiver de acordo com a política de segurança da empresa. Algumas vezes os guardas guardam informações do visitante (anotam o nome e R.G. do visitante, tiram fotos, etc.) mesmo que ele não tenha permissão de entrar.

Como um guarda na entrada de um edifício, o Firewall é colocado na entrada da rede de computadores ou na entrada da Intranet corporativa. Para fazer corretamente o seu trabalho todo o tráfego deve passar por ele; isso o torna, inevitavelmente, um potencial gargalo na rede e se o Firewall não for dimensionado corretamente irá causar atrasos e diminuir a performance da rede.

A figura 8 mostra uma configuração típica de uma rede com Firewall.

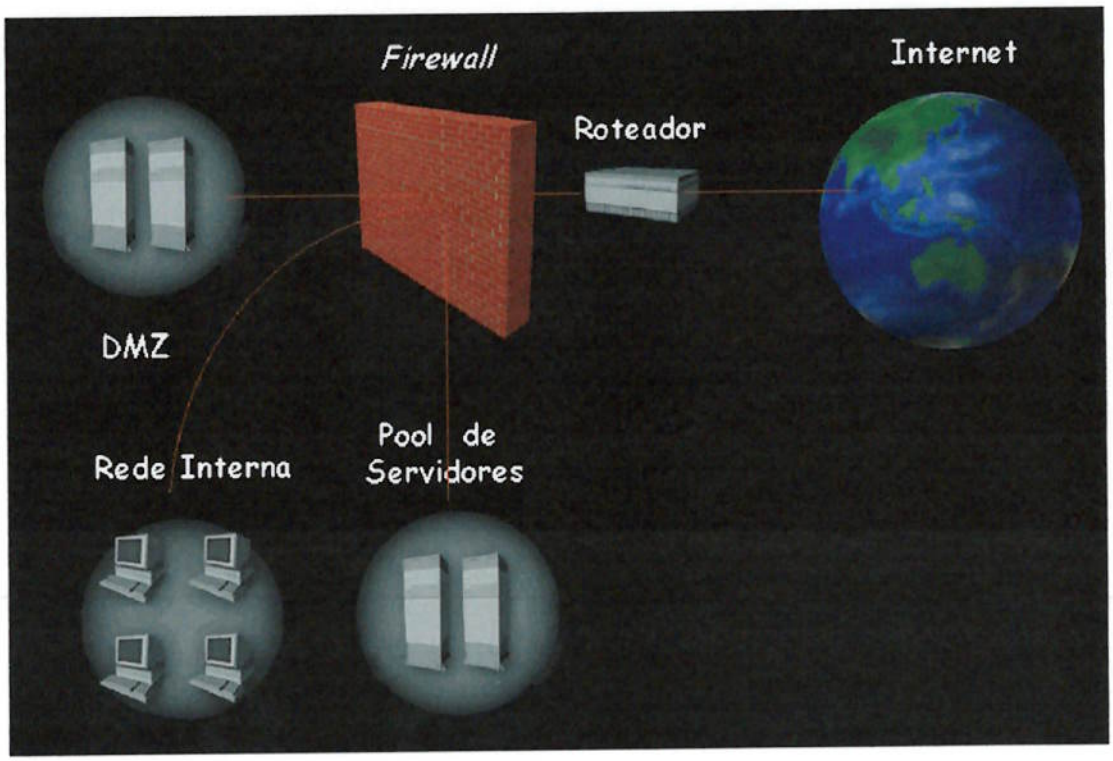

Figura 8 – Configuração Típica de rede com Firewall

3.4.2 Tipos de Ameaça à Segurança

Durante os primeiros anos, os especialistas de segurança estavam quase totalmente focados nas ameaças vindas de fora. Eles estavam preocupados com hackers ou espiões industriais ou mesmo ameaças de governos estrangeiros. Eles não deram muita atenção ao pessoal interno. Muitos acreditavam que se eles tivessem um bom Firewall entre a sua rede e o mundo exterior eles estariam seguros. As corporações freqüentemente ignoram o simples fato de que nenhum Firewall localizado entre a rede e o resto do mundo poderá protege-las contra certos problemas.

Mais importante: nenhum Firewall que controla apenas o acesso externo à rede pode proteger contra hacker internos.

Se a organização necessita proteger-se contra ataques vindos de fora como de dentro da empresa ela deve configurar vários Firewalls, um para se proteger contra os invasores vindos da Internet e outros, em vários pontos da Intranet, para minimizar as oportunidades de funcionários obterem informações que eles não deveriam.

Nos últimos anos, novos serviços de rede tem complicado os problemas de segurança ainda mais. Um deles é a Extranet. Uma Extranet liga duas ou mais companhias diretamente, através das Intranets corporativas, de forma que elas possam se comunicar de maneira mais eficiente.

Isso impõe novos tipos de ameaças à segurança: empregados descontentes de uma empresa ganhando acesso à rede de computadores da outra empresa e roubando ou corrompendo informações. A solução: colocar Firewall entre as Extranets para proteger as informações confidenciais do ataque de funcionários da outra empresa [Strebe e Perkins, 2002].

E tem também o e-commerce. Alguns especialistas acreditam que o e-commerce será a maior e mais importante aplicação de todas na Internet, fornecendo uma nova maneira das empresas fazerem negócios com outras empresas e pessoas. Mas se as empresas e pessoas não tiverem confiança nas transações pela Internet o e-commerce não terá sucesso.

Um forte e bem posicionado Firewall pode ser o único meio de obter a segurança necessária.

Para determinar as suas necessidades, uma empresa considerando a aquisição de um sistema de Firewall deve fazer a si mesma as seguintes questões:

Quais as informações importantes que nós temos? Obviamente uma usina nuclear tem um patrimônio de informações e necessidades de segurança bem diferentes de uma loja de departamentos.

Quão críticas são essas informações? Para algumas corporações a questão deve ser: devemos realmente estar conectados? Uma usina nuclear é um exemplo. Para essas empresas o melhor de todos Firewall é não ter conexão física ou elétrica nenhuma. Mas esse é preço muito alto a ser pago para empresas em geral.

Quão atrativa é sua informação para os invasores? Algumas empresas são alvos naturais de invasores: órgãos do governo, bancos, grandes corporações, para citar apenas alguns. Outras empresas menos conhecidas não são alvos tão freqüentes de ataques.

Quais os tipos de serviços serão utilizados pelos clientes e empregados? É o e-mail o serviço mais importante? Ou o acesso à páginas Web? É importante saber, porque os tipos de serviço que os clientes e empregados irão necessitar determinarão o tipo de tráfego que o Firewall irá gerenciar.

Os sistemas de Firewall disponíveis comercialmente se diferenciam de duas maneiras: seu conjunto de características e sua arquitetura básica .

Arquitetonicamente, os Firewalls estão disponíveis em três tipos:

O Firewall filtros de pacotes: no seu projeto, dados – os pacotes IP – chegam até ele que decide se os passa ou não para a rede, dependendo de regras de filtragem embutidas em seu sistema operacional. Este projeto é considerado o mais rápido e flexível dos dois.

O Firewall a nível de aplicações: esse tipo de projeto não permite que nenhum pacote passe diretamente entre a rede externa e a rede corporativa. Ao invés disso todos os pacotes são enviados a uma servidor de proxy. O proxy determina quando se deve ou não estabelecer a conexão. Este sistema é mais lento que o filtro de pacotes e mais inflexível; o proxy tem que conhecer a aplicação e, se uma nova aplicação for necessária na rede, deve obter com o fornecedor um novo código que a contemple.

O híbrido: nesse sistema estão inclusos elementos dos dois tipos anteriores de projeto para maximizar segurança e performance.

3.4.3 Características Básicas

Os sistemas de Firewall disponíveis hoje em dia vem com quase todas as possíveis combinações de características. Algumas são essenciais, outras necessárias apenas em circunstâncias especiais.

Controle de acesso básico: Essa é a razão de ser do Firewall, controlar o acesso à rede. Mas alguns Firewall oferecem controles de acesso que são mais poderosos, fáceis de administrar e difíceis de burlar.

Serviços suportados: Isso se refere aos protocolos, no nível de aplicação, que o Firewall reconhece e passa. Um Firewall a nível de aplicação deve ter um serviço de proxy para cada uma. Os Firewalls filtros de pacotes suportam todos os serviço. Entre os serviços mais conhecidos temos: DNS, Finger, FTP, Gopher, ICMP, IRC, Mail, Telnet e, é claro, WWW ou World Wide Web.

Autenticação de usuários: Os Firewalls a nível de aplicação normalmente utilizam esse conceito, interrompendo aplicações e exigindo dos usuários que se autentiquem antes de continuarem a conexão no destino requisitado. Alguns serviços permitem isso: Telnet, FTP, X11 e HTTP. Alguns outros não.

Redes privadas virtuais: as VPNs estão se tornando cada vez mais populares. Como o Firewall é a porta de entrada da corporação nada mais natural do que utiliza-lo como servidor das VPNs e ser o responsável pela autenticação dos usuários.

Administração: uma corporação pode ter um Firewall de primeira linha e uma política de segurança bem restrita e ainda assim sofrer um sério ataque. Por que? Porque o administrador do Firewall, como qualquer humano, comete erros. Infelizmente isso é bastante comum pois os Firewalls estão se tornando cada dia mais complexos e complicados de administrar. Uma solução para o problema: uma interface gráfica com bons recursos de auxilio ao operador que permitam que mesmo uma pessoa não especialista possa gerenciá-lo facilmente.

Auditoria e alarmes: os administradores de Firewall devem ser notificados quando alguém tenta invadir a rede. Eles precisam saber que tipo de ataque está sendo direcionado contra eles de forma que eles possam aumentar a segurança contra o ataque e o atacante. Eles também necessitam saber, quando possível, exatamente quem está atacando. Se essa informação for disponibilizada em tempo real o administrador do Firewall tem mais chances de identificar o potencial invasor.

Alta performance: Firewalls lentos podem ser um sério gargalo na rede. Isso não era importante no passado já que poucas empresas tinham conexões rápidas com a Internet. Nos dias de hoje a performance do Firewall deve ser considerado pois conexões de alta velocidade com a Internet estão se tornando cada vez mais comuns. Muitos Firewalls no mercado simplesmente não estão prontos para essa tarefa.

Mapeamento de endereços: Antes do crescimento explosivo da Internet, muitas organizações tinham redes de computadores privadas sem conexão com outras redes. Elas simplesmente não tinham necessidade de conexão com a Internet e por isso não tinham endereços IP válidos na Internet, utilizavam o endereçamento da forma que era mais apropriada. Hoje essas organizações estão se ligando à Internet e descobrindo que os endereços que eles utilizavam já pertencem a alguém. Alguns Firewalls resolvem esse problema trocando, dinamicamente, os endereços ilegais pelos endereços legais quando os pacotes saem para a Internet em uma operação chamada NAT.

Controle de quantidade máxima de conexões permitidas: Essa característica ajuda a evitar ataques do tipo sobrecarga da rede, os chamados "flooding attacks".

3.4.4 O Futuro dos Firewalls

Diariamente temos notícias de sites que foram invadidos ou do surgimento de novas ameaças de segurança. Isso sem contar o fato de que muitos ataques não são divulgados ao público porque as corporações atacadas temem a publicidade negativa e de expor suas vulnerabilidade em público.

Como resultado, muitas corporações e empresas estão relutantes em colocar suas informações cruciais na Intranet da companhia ou disponibilizar acesso à Internet por toda a empresa com medo de criar sérios problemas de segurança. Muitos usuários também estão preocupados. Por exemplo, alguns são relutantes em fazer compras via Internet utilizando cartões de crédito porque não estão confiantes o suficiente nas medidas de segurança utilizadas.

Os Firewalls são claramente uma parte essencial de qualquer solução de segurança de rede hoje. Para fornecer máxima proteção contra invasão eletrônica e, ao mesmo tempo permitindo novas aplicações de comércio eletrônico, é importante que os Firewalls operem como parte de uma plataforma de segurança integrada.

3.5 IDS - Intrusion Detection System

O IDS tem como objetivo detectar atividades impróprias, incorretas ou anômalas, sendo capaz de alertar (detectar) aos administradores quando a possíveis ataques ou comportamentos anormais na organização.

Se alguém invadir a sua rede, como você vai saber? Não haverá nenhuma pegada. Se você tiver um bom Firewall com bons recursos de registro de ocorrências, poderá encontrar evidências de um ataque nos registros, embora um hacker esperto possa evitar isso.

Para montar um sistema de detecção de invasão rigoroso, além do que é fornecido pelos Firewalls e seus registros, considere o caso de um verme Internet típico: um funcionário recebe uma mensagem de e-mail da conta pessoal de um colega de trabalho dizendo que ele encontrou uma cópia de um arquivo que havia desaparecido faz alguns meses. O funcionário dá um clique então no anexo executável que diz ser

um arquivo Zip e acaba instalando um cavalo de Tróia sem saber. Ele fica a espera até detectar um período de inatividade de teclado e de mouse grande o suficiente para considerar que o funcionário não está olhando para o computador e então abre uma conexão com o computador de um hacker. Mesmo se o Firewall fosse projetado para bloquear conexões dirigidas para fora através de portas incomuns, e a grande maioria não o é, nada impediria que o hacker usasse em seu software de ataque uma porta comum como a 80 (HTTP). O Firewall iria simplesmente ver o que parece ser uma conexão HTTP para fora da rede dirigida para um servidor Web, um tipo de conexão que ele vê milhares de vezes por mês [Strebe e Perkins, 2002].

Mesmo nesse caso, um hacker inteligente poderia simplesmente usar uma porta de dados binários como a usada pelo FTP que somente pode filtrar os dados de conexão iniciais; o arquivo real de dados binário não pode ser filtrado, porque não há como prever o que o arquivo deveria conter. O hacker projeta o cavalo de Tróia e o servidor de ataque de modo que transmita dados de estabelecimento de sessão falsos, enquanto o cliente parece estar apenas transmitindo um arquivo, mas está na verdade transmitindo imagens de tela e aceitando entrada de mouse e de teclado. Um cavalo de Tróia bem projetado poderia até mesmo trabalhar usando um proxy FTP. Qualquer outro protocolo binário também poderia ser explorado. Se você confiar nos registros de ocorrências de um Firewall para saber quando ocorreu uma invasão, nunca encontrará esse tipo de ataque porque para o Firewall ele se parece com uma sessão de transferência de arquivos via FTP normalmente iniciada. Nada sobre essa sessão acionará qualquer aviso ou alarme.

Dessa maneira, concluímos que mesmo os Firewalls mais eficientes não podem evitar certos ataques. Qualquer conexão funcional com a Internet é um vetor em potencial para um ataque.

Veremos agora como proteger uma rede contra os ataques que o Firewall não pode evitar, como determinar quando está ocorrendo o ataque ou, mais importante, quando o ataque está ocorrendo e como avaliar a extensão dos prejuízos caso ocorra uma invasão bem sucedida. Examinaremos algumas técnicas de detecção de invasões que podem ser usadas sem gastar mais dinheiro com software especializado, bem como alguns dos pacotes de software principais disponíveis para detecção de invasão.

A figura 9 a seguir mostra uma configuração básica de uma solução de detecção de intrusão.

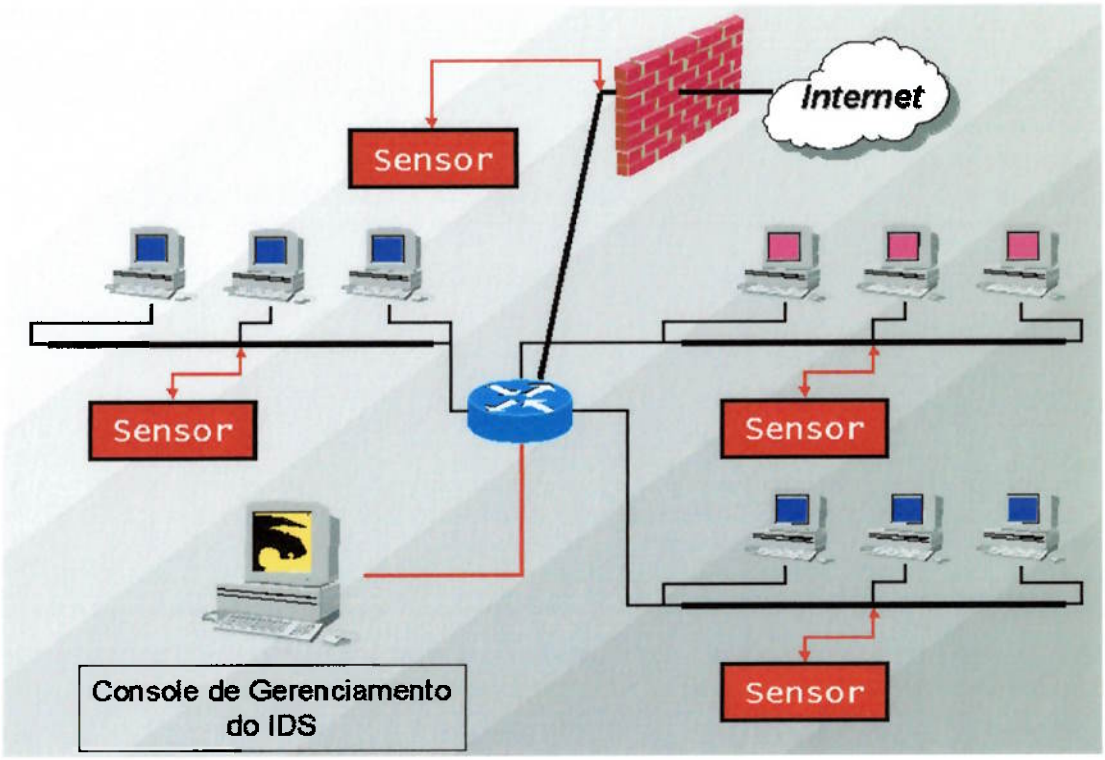

Figura 9 – IDS em uma Rede Corporativa

3.5.1 Problemas incomuns de invasão

Nos preocuparemos principalmente com a detecção de invasão em uma rede a partir da Internet. Mas, antes que possamos ver a detecção de invasão de TCP/IP e de camada de aplicação, é importante entender que uma invasão pode considerar várias formas em muitas outras camadas de uma rede.

Notoriamente, os hackers são caras-de-pau, e são conhecidos por entrarem em uma empresa para obter dados diretamente ou instalar software que lhes permita uma penetração posterior mais aprofundada na rede.

Se a empresa tem segredos que valham a pena serem roubados, há agências de espionagem estrangeiras conhecidas por não medirem esforços para adquirir informações em seu interesse nacional. Muitos governos estrangeiros pedem a seus

agentes que adquiram informações de interesse econômico para seus negócios mais importantes.

As medidas nesse caso são extremamente raras; a maior parte das empresas não precisa se preocupar seriamente com a segurança física. Mas, se sua empresa realiza qualquer atividade de pesquisa e desenvolvimento, então deverá usar uma política de segurança mais rígida para proteger o produto das pesquisas.

A prevenção de uma invasão real começa com a segurança das condições básicas, a segurança da camada física e a segurança da camada de enlace de dados. Se uma rede for tão fortificada contra ataques pela Internet que um inimigo dedicado não consiga passar pelas defesas, este irá simplesmente mudar de tática e tentar invadir diretamente.

3.5.2 Ferramentas e técnicas de invasão

Os hackers usam uma variedade de técnicas e ferramentas para atacar as redes. Uma invasão típica toma a seguinte forma, considerando que o hacker comece sem nenhuma informação sobre o site alvo a não ser seu endereço:

Varreduras de endereços

Varreduras de portas

Avaliação de serviços

Seleção de alvos

Sondas de vulnerabilidades

Ataques automatizados de senhas

Ataques incomuns

Varreduras de endereços - Significa percorrer o intervalo de endereços de uma rede para descobrir hosts que oferecem serviços. Os hackers geralmente procuram em todo o intervalo da classe C de endereços IP ao redor do host e podem usar pesquisa

de DNS reversa para determinar se esses outros hosts são registrados na empresa. Por esse motivo, você deve considerar que eles irão descobrir os hosts públicos existentes na Internet, mesmo se seus endereços não forem públicos.

Varreduras de portas - Significa analisar os hosts que respondam à procura de serviços sendo executado neles. Essa informação diz ao hacker que serviços estão sendo executados em cada host de acesso público. As varreduras de portas normalmente passam pelos Firewalls enquanto um host puder ser alcançado, especialmente se a varredura se limitar a portas de serviço como a 21 e a 870 em vez de percorrer todas as portas, o que alguns Firewalls são capazes de detectar imediatamente e impedir.

Avaliação de serviços - Significa determinar o tipo de sistema operacional de cada host. Após sondar as portas dos serviços mais comuns, como Echo, Charge, FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, serviço localizador de RPC, NetBIOS, NFS etc., o hacker irá determinar que sistema operacional cada host parece estar executando. Hosts com base em Windows em geral respondem nas portas NetBIOS mas não respondem na porta Telnet, enquanto os hosts UNIX respondem na Telnet mas não no serviço localizador de RPC usado pelo Windows NT. Os hosts Linux em sua configuração padrão respondem a uma ampla gama de serviços e são mais fáceis de reconhecer por esta razão.

Seleção de alvos - Significa selecionar os hosts mais fracos encontrados. Os hackers geralmente escolhem como alvo o host com mais serviços operando na suposição de que pouco ou nada foi feito para mudar ou proteger a configuração padrão desse host. Os hosts Windows que respondem na porta 139 (NetBIOS) serão alvos de ataques certos, pois por meio desse serviço você pode conseguir controlar totalmente uma máquina.

Sondas específicas de serviços - Significa usar ferramentas de análise de vulnerabilidade como o SATAN em sistemas UNIX ou o Internet Scanner da ISS (Internet Security Systems) em Host Windows. Essas sondas inspecionam uma ampla gama de vulnerabilidades conhecidas de serviços que são fáceis de explorar e que por isso são examinados primeiro.

Ataques automatizados de senhas - São ataques usados contra serviços como FTP, HTTP, NetBIOS ou outros que permitem acesso ao sistema de arquivos. Os hackers usam software escrito especificamente para realizar uma alta taxa de tentativas de acesso de entrada, como a de NetBIOS Auditing Tool, usando dicionários de senhas mais comuns. Se esse ataque falhar, a maior parte dos hackers desistirá ou então passará para ataques do tipo recusa de serviço se ele tiver realmente algo contra você.

Se um hacker tiver acesso ao console de uma máquina, certamente executará um quebrador *(crackery)* de senhas automatizado como o Crack ou o NT Crack contra seu host para explorar outras contas. Os hackers também são conhecidos por configurarem sites Web chamarizes oferecendo utilitários de graça para descobrir nomes de usuário e senhas. Eles obtêm o endereço IP do visitante e, se este digitar um nome e uma senha de conta, o software poderá associar a conta e o endereço IP, de modo que eles passam a saber onde você está e que identificação gosta de usar. Você sempre usa o mesmo nome de usuário e senha ao trabalhar nos sites Web? como na Technet da Microsoft? ou nos milhares de sites de suporte para software de rede? A maioria das pessoas sim. Isso torna fácil para os hackers descobrir seu nome de usuário e senha preferidos.

Ataques incomuns - Abrangem o conjunto restante de ataques que um hacker poderia empregar, incluindo as táticas incomuns e difíceis que os hackers poderiam usar se eles realmente quiserem explorar determinados servidores Internet e nenhuma das técnicas anteriores tiver funcionado. Esses ataques incluem ataques de roteamento de origem, tentativas de seqüestro, escuta clandestina de rede à procura de senhas ou e-mail chamariz para instalar um cavalo de Tróia. Esses ataques são excepcionalmente raros.

Os hackers empregam uma ampla gama de ferramentas de software em suas atividades. Ferramentas projetadas para administradores de rede, como SATAN e Internet Security Scanner, tornam-se armas poderosas nas mãos de um bom hacker.

Os hackers também gostam de explorar ferramentas de software específicas usadas em uma rede. Por exemplo, os Firewalls usados nas empresas sempre têm aplicativos para gerenciamento remoto, a maior parte dos quais se baseia em uma senha secreta

compartilhada única e pequena. Além disso, muitos Firewalls têm "regras secretas" que permitem a conexão do seu software cliente de gerenciamento remoto na percepção errônea de que você sempre desejará gerenciar remotamente o Firewall. Quase todos os Firewalls que examinamos podem ser baixados gratuitamente pela Internet em versões de avaliação. Embora o programa do Firewall só opere durante o período de avaliação, digamos, 60 dias, a interface de gerenciamento funcionará sempre. E isso significa que todos os hackers do planeta têm as ferramentas de gerenciamento remoto desse Firewall; tudo de que eles precisam é da senha.

3.5.3 Sistemas de detecção de invasões

Os sistemas de detecção de invasões são sistemas de software que detectam invasões em uma rede com base em um certo número de sinais reveladores. Os sistemas de resposta ativa tentam ou bloquear os ataques, ou responder com contramedidas ou pelo menos alertar os administradores que está ocorrendo um ataque. Já os sistemas de IDS passivos apenas registram a invasão ou criam registros de ocorrências que só aparecem depois que o ataque aconteceu.

Embora os sistemas passivos possam parecer ineficientes ou de certa forma inúteis, há diversos indicadores de invasão que somente aparecem depois que a invasão ocorreu. Por exemplo, se um administrador de rede ressentido decidir atacar, ele terá todas as chaves e senhas necessárias para acessar de imediato. Nenhum sistema de resposta ativo poderia emitir nenhum alerta nesse caso. Por outro lado, os sistemas de IDS passivos podem detectar as alterações que esse administrador fizer nos arquivos de sistema, as remoções ou quaisquer prejuízos que possam ter causado.

3.5.4 Detectores de invasões com base em inspeção

Os detectores de invasões com base em inspeção são o tipo mais comum. Esses detectores observam o modo da atividade em um host ou em uma rede e decidem se está ocorrendo ou se ocorreu uma invasão com base ou em regras programadas ou em indicações históricas de uso normal. Os detectores de invasões incluídos em Firewalls e em sistemas operacionais, bem como a maioria dos detectores de invasões independentes e disponíveis comercialmente, se baseiam em inspeção.

Os detectores de invasões fazem uso de indicadores de uso inadequado. Esses indicadores incluem:

Tráfego da rede, como varreduras de ICMP, varreduras de portas ou conexão a portas não autorizadas.

Utilização dos recursos, como CPU, RAM ou surtos de uso de E/S da rede em horários inesperados. Isso pode indicar um ataque automatizado contra a rede.

Atividade de arquivos, incluindo arquivos criados recentemente, modificações de arquivos do sistema, mudanças nos arquivos de usuários ou modificação das contas de usuários ou das permissões de segurança destes.

Os detetores de invasões monitoram as várias combinações desses sinais reveladores e. cria entradas em um registro de ocorrências. O corpo desse registro e chamado de trilha de auditoria , que consiste no acúmulo de parâmetros observados de um certo objeto de acesso ,como uma conta de usuário ou um endereço IP de origem. Os Sistemas de detecção de invasão podem monitorar as trilhas de auditoria para determinar quando as invasões ocorrem.

Os sistemas de detecção de invasão podem ser:

Com base em regras - Detectores de invasões que se baseiam em seqüências de atividades de usuários chamadas regras que reconhecidamente indicam tentativas de invasão, como varreduras de portas, modificações de arquivos do sistema ou conexões a certas portas. A maioria dos sistemas de detecção de invasão se baseia em regras.

Estatísticos - Detectores de invasões que as detectam comparando a base existente de trilhas de auditoria válidas com cada nova trilha de auditoria. As trilhas de auditoria que diferirem substancialmente da norma são marcadas como possíveis tentativas de invasão. Sistemas como este têm a capacidade de detectar métodos de intrusão até então desconhecidos, mas também podem deixar passar invasões óbvias que se pareçam com uso normal.

Híbridos - Os sistemas de detecção de invasões híbridos são os que oferecem o melhor dos dois mundos, combinando os métodos estatísticos com os de base em regras. Alguns destes sistemas são capazes de criar novas regras permanentes a partir de invasões detectadas para evitar que ocorram novamente sem sobrecarregar ou depender da análise estatística.

Os sistemas de IDS sempre exigem recursos do sistema para operarem. Os sistemas de IDS de rede geralmente são executados em Firewalls ou em computadores dedicados; isso geralmente não é um problema, porque há recursos disponíveis. Contudo, sistemas de IDS com base em hosts projetados para proteger servidores podem ser um sério impedimento.

Os sistemas de IDS com base em regras somente podem detectar vetores de invasão conhecidos, assim nem todas as invasões podem ser detectadas. Os detectores de invasões por métodos estatísticos sustentam que têm maiores possibilidades de detectar vetores desconhecidos, mas não podem provar isso a não ser depois do fato.

Devido a essas limitações, os sistemas de IDS geralmente precisam do monitoramento de administradores de segurança humanos para serem eficazes. A tecnologia de contramedidas e sistemas de resposta que aumentam temporariamente a postura de segurança do host durante ataques estão todos no estágio I da pesquisa teórica. Os sistemas de IDS atuais dependem de alertar administradores humanos sobre a presença de um ataque, o que torna os administradores humanos parte ativa do sistema de detecção de invasões.

3.5.5 Detectares de invasões por isca

Os detectores de invasões por isca operam imitando o comportamento expressivo de um sistema alvo, mas em vez de fornecer um vetor de ataque para o hacker, eles alarmam sob qualquer ocorrência de uso. As iscas se parecem com um alvo real que não foi protegido apropriadamente.

Quando um hacker ataca uma rede, ele faz uma série metódica de ataques bem conhecidos, como as varreduras de endereços de portas, para determinar que hosts estão disponíveis e que serviços esses hosts fornecem. Com hosts ou serviços iscas

você pode atrair o hacker a atacar um host ou um serviço que não é importante mas que é projetado para servir de alarme.

As iscas podem operar como um único serviço em um host em operação normal, como uma variedade de serviços armadilhas em um host em operação normal, como um host isca ou como toda uma rede chamariz. As redes chamarizes são muito raras. A maior parte do software isca executa em um host Chamariz.

A padronização do IDS é um processo que ainda esta em andamento e tem como objetivo criar formatos e procedimentos para compartilhamento de informações entre os sistemas.

O IDS ao detectar tentativas de ataques externos e internos, dependendo da localização, permite que o administrador de segurança tenha conhecimento sobre o que esta acontecendo e sobre qual medida tomar com relação ao ataque, sempre agindo de acordo com a política de segurança da empresa.

3.6 Backup

Até profissionais de informática não dão muito importância a este tema. Com poucos, não é possível argumentar e estes só aprendem depois de uma experiência pessoal dolorosa. Felizmente, a grande maioria se convence da importância do *backup* ao lhes fazer uma simples pergunta: qual seria a sua reação ou prejuízo se você perdesse informações do seu HD que eram os resultados de uma semana inteira de trabalho? Faça a si mesmo esta pergunta. Se com uma semana perdida o impacto não é tão grande no seu caso, então aumente para um mês.

Geralmente quando se utiliza muito as facilidades de um PC, produz-se muita informação em apenas um dia de trabalho. É importante ressaltar que não é necessário se preocupar com os programas instalados em sua máquina, pois todos podem ser reinstalados a qualquer momento. A maior importância deve ser dada aos seus dados pessoais e personalizados. Aquelas cartas e pensamentos que estão guardados há um ano em seu HD, planilhas utilizadas na semana passada mas que podem vir a ser necessárias novamente, aqueles gráficos que alguém passou horas

aperfeiçoando pixel por pixel, enfim, a rotina de *backup* ou *cópia de segurança* é indispensável em 99% do casos.

Pior do que não ter um *backup* na hora de um desastre é ter uma rotina organizada com várias cópias de segurança, porém com discos que contenham falhas ou com a gravação errônea dos dados, impossibilitando em parte ou totalmente a recuperação dos dados. Quem estava tranqüilo pode acabar ficando transtornado com a falsa segurança. Assim como é importante a cópia dos dados para as mídias de segurança, é essencial a verificação do funcionamento do caminho inverso, ou seja, a restauração dos dados das mídias externas para as de uso corrente.

Convém lembrar, principalmente aos administradores de rede, que por melhor que eles se desempenhem e por mais qualificação técnica que tenham, que existem dois fatores cruciais que diferenciam um administrador regular ou bom de um ótimo: rotina de backup que inclui a restauração periódica dos dados para verificação, monitoração e análise comparativa periódica do desempenho da rede. Pode-se afirmar que o backup consiste em duas operações, a ida e a verificação da volta dos dados. Uma rotina que só engloba a gravação dos dados em mídias pode-se chamar de meio backup [Redes, 2000].

3.6.1 Tipos de Backup

Dependendo dos nossos interesses deve-se escolher um determinado tipo de backup ou associação dos tipos abaixo.

Cópia Simples

Cópia dos arquivos desejados sem nenhuma alteração e nem com modificação de atributos dos mesmos; não envolve compressão ou classificação de dados.

O Windows marca arquivos modificados com o atributo *"arquivo"*. Alguns programas de backup compreendem este tipo de sinalização.

Normal

Cópia de todos os arquivos que foram selecionados sem considerar o atributo de arquivo dos dados; limpa os atributos de *arquivo* de todos arquivos copiados, a fim de indicar que foram copiados.

Diária

Este método faz a cópia verificando a data dos arquivos; existindo arquivos com data de modificação coincidente com a do dia da cópia em procedimento, estes são copiados sem a necessidade de alteração de seus atributos.

Diferencial

Copia apenas os arquivos que sofreram modificação desde a última cópia normal. É um método que economiza tempo e que deve ser usada em conjunto com o modo normal. Os atributos dos arquivos não são mudados, sendo assim, uma cópia diferencial de quinta-feira contém as mudanças feitas, por exemplo, da cópia de terça até quinta.

Incremental

É parecido com o método anterior. Consiste na copia apenas dos arquivos selecionados que tiveram seus atributos mudados desde o último backup normal. Limpa os atributos de arquivo dos arquivos para indicar que foram realmente copiados. É um método que também visa a economia de tempo. A diferença é que havendo a necessidade de recuperação dos dados na quinta-feira, precisaremos recuperar os dados do backup normal e de cada backup incremental feito depois do normal e antes de quinta-feira. É mais rápido que a cópia diferencial.

3.6.2 Tipos de Mídia

Não se deve esquecer que as mídias magnéticas, que dominam as soluções de backup existentes, retêm os dados por poucos anos, ou por um número limitado de regravações. Devido a isto deve-se usar um grupo de mídias em regime de rodízio (rotação), para minimizar possíveis. É aconselhável a marcação na própria etiqueta

da mídia, o número de vezes ou as datas em que esta foi utilizada. Ao longo do tempo estas mídias devem ser repostas por novas.

Deve-se usar um conjunto confiável de mídias, uma para cada dia de semana, uma para cada semana, uma para cada mês, uma para cada ano e sucessivamente conforme a necessidade, emprego e durabilidade das mídias. As ilustrações da figura 10 representam procedimentos combinados e rotação das mídias que são válidos para uma rotina segura de backup.

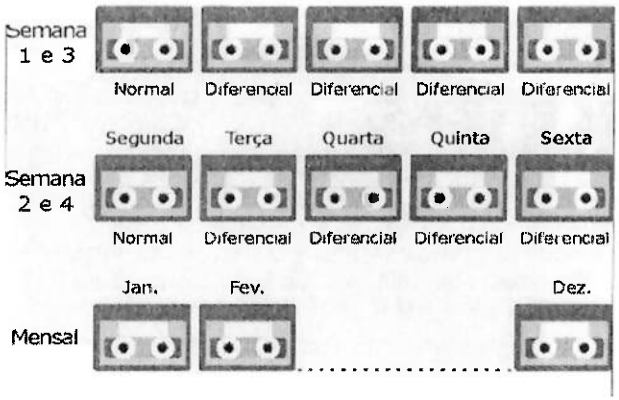

Figura 10 - Sistema de rodízio de mídias para backup

Mesmo estando totalmente satisfeitos com os procedimentos de backup, sabemos que os dados podem ser alterados a cada segundo. Sendo impraticável um backup neste freqüência de atualização, é recomendável usar em conjunto com o procedimento de backup testado e aprovado, tecnologias oferecidas pelos sistema operacionais e hardware especiais, como RAID e o serviço de replicação de diretórios.

Hoje em dia conta-se com muitos modelos de mídias para backups. Estes modelos se baseiam em dois métodos distintos: gravação magnética e gravação óptica ou magneto-óptica. Conforme a quantidade das informações, velocidade desejada, custo e confiabilidade têm-se diversas soluções.

Meios Magnéticos

Os meios magnéticos em rolos de fita, por mais rápidos que sejam, não são a melhor opção para o futuro. Devido a seu acesso seqüencial. Por exemplo, para chegar até uma informação que está no fim da fita, é necessário passar por toda a fita. Mídias

com este tipo de acesso estão, gradativamente, sendo substituídas por aquelas com técnicas de acesso randômico.

Um dos primeiros tipos de fitas magnéticas empregadas para backup foram fabricadas em 1972 pela 3M e chamava-se QIC (Quarter lnch Cartdrige).

Atualmente o tipo mais comum de gravação por fita são os drivers de fita DAT, Digital Áudio Tape, que ainda são muito usados em soluções de backup apesar de suas mídias terem uma curta vida útil. A fita DAT é similar a uma fita cassete de áudio, porém contêm um comprimento muito maior de filme magnético podendo chegar até mais de 150 metros. A técnica utilizada nestas fitas, conhecida como busca helicoidal foi herdada da indústria de fitas de vídeo. Basicamente existem dois grupos de fitas DAT: 8mm e 4mm.

Há fitas de 8 mm criadas criada pela Exabyte. Seu padrão foi copiado das fitas Betamax de vídeo, criadas pela Sony: Estas fitas atingiam no máximo 5 GB (10 GB comprimidos), porém com o advento das fitas de 4 mm esta categoria ficou obsoleta.

As fitas de 4 mm tem o formato das fitas DAT de áudio, criadas pela Sony. Suportam altas capacidades de armazenamento e boas taxas de transferência seqüencial. Os drives podem ofertar 4,8 MB/s com fitas DDS-4 de capacidade máxima de 40 GB, como o modelo SDT- 10000 da Sony.

Também há as DLT, Digital Linear Tape, criadas em 1980 com capacidades já atualizadas para 80 GB. Uma variação é a Super DLT, criada em 1999 e com capacidade de até 500 GB. Um outro tipo é a AIT, Advanced Intelligent Technology, que comporta até 50 GB. Há ainda a AIT- 2 de 1996, ADR, Advanced Digital Recorder, de 1999 e LTO, Linear Tape Open. É possível encontrar sistemas autocarregáveis que se utilizam de algumas fitas em conjunto e de bibliotecas que são verdadeiros carrosséis de fitas. Eles podem suportar dezenas de fitas e alternar automaticamente entre uma e outra. Estes dispositivos possuem alta capacidade de armazenamento. Atualmente com o uso das DLT em bibliotecas, chega- se a capacidades de 19,1 TB e com o emprego de mídias AIT chega-se a 46,98TB.

Meios Ópticos

Eles provêm maior vazão dos dados, sendo que suas mídias possuem maior vida útil, apesar de requisitarem cuidados mínimos. Pode-se dividir este grupos em outros subgrupos.

Magneto Ópticos

Combinam a tecnologia do laser e da gravação magnética. Usa um feixe laser para polarizar um filme magnético. Não é a melhor opção a ser considerada.

Gravação Única

São designados para grandes quantidades de dados. Usa-se o laser para marcar a superfície de um polímero especial. As mídias possuem longa vida útil principalmente por serem imunes a campos eletromagnéticos externos. Não são mídias regraváveis.

Múltiplas Gravações

Este é o caso mais interessante, pois estas mídias óticas podem ser gravadas e regravadas, respeitando- se um limite obviamente. Uma das melhores soluções neste caso é o uso de gabinetes e carrosséis, que se utilizam de diversas mídias que se revezam automaticamente, sendo que estas não são manuseadas e nem ficam em contato com o meio externo aumentando ainda mais a vida útil das mídias. Um exemplo desta categoria é o CD-RW. Têm-se hoje em dia as mídias DVD *(Digital Versatile Disc)* que suportam mais informações que os CDs, 17 GB contra 650 MB, cerca de 26 vezes mais, porém as soluções de backup com o uso destas mídias ainda não estão acessíveis.

4 CONCLUSÃO

Como visto no capítulo anterior existe uma série de ferramentas de mercado que, se bem selecionada e implementada, garante um bom nível de segurança.

A seleção de um determinado produto ou ferramenta deverá ser um passo complementar das etapas de detecção de vulnerabilidades e análise de riscos.

A detecção de vulnerabilidades tem como objetivo descobrir pontos falhos no ambiente, principalmente aqueles provocados por sistemas desatualizados no que diz respeito à segurança, ou seja, apontarão os sistemas operacionais de servidores, de equipamentos de conectividade como roteadores ou switches que não foram objeto de correção ou de implementação sugeridas pelos fabricantes através do chamados patches; outra falha que poderá ser detectada é o do de uso de senhas fracas ou óbvias nos serviços de autenticação.

A relação de vulnerabilidades será um dos componentes da análise de riscos que apontará onde deverão ser investidos recursos de modo a minimizar o risco de ocorrência de segurança. Para tanto, é importante quantificar o valor das informações a serem protegidas para confrontá-lo com o custo das soluções no caso de compra e implementação das soluções tecnológicas apresentadas. Sem essa análise, pode ocorrer de se adotar uma solução de segurança com custo superior ao valor do que se pretende proteger.

Uma vez decidido por um determinado tipo de solução que deverá ser compatível e aderente ao ambiente da corporação, ambiente esse que engloba os serviços (servidores, sistemas operacionais), o sistema de comunicação e o parque de estações de trabalho, passa-se ao processo de seleção entre as ferramentas disponíveis no mercado. Na decisão dessa escolha, além dos requisitos técnicos, devem ser considerados requisitos como suporte, níveis de serviço (SLA - Service Level Agreement), facilidades de implantação, configuração e operação, aderência a padrões e, sempre que possível, solução consolidada no mercado. Quando da implementação da ferramenta é sempre recomendável a ativação somente dos parâmetros e recursos indispensáveis ao pleno funcionamento das funções desejadas;

a razão está no fato de que quanto maior o número de opções ou "aberturas" nos sistemas, maior a probabilidade de ocorrência ou existência de falhas (bugs), aumentando consideravelmente as possibilidades para os oportunistas.

Deve-se considerar que tão importante quanto a ferramenta em si é a definição e formalização de regras e procedimentos que norteiem a correta operação e o bom aproveitamento da solução adotada. Como exemplo, pode-se citar o caso de uma ferramenta de backup: ela só será justificada se quando dela se precisar ela cumpra o seu papel que é o de permitir a rápida restauração da informação; isso será possível se houver documentos formalizados que definam, por exemplo, o que e quem deve executar as atividades básicas de um sistema de backup como a gravação da informação e, quando necessária, a sua recuperação que é a sua razão de ser.

Outra consideração refere-se a aspectos ético legais que determinada solução pode implicar. Ao se adotar, por exemplo, ferramentas de monitoração de navegação na Internet e, mais sensível ainda, monitoração de correio eletrônico, vem à tona a questão da privacidade, um assunto bastante atual. No caso do correio eletrônico, há, por um lado, o grupo de pessoas que se alinha ao pensamento de que não existindo lei específica que restrinja aquele ato e considerando que são utilizados recursos da empresa e, portanto, desde que respeitados princípios ético legais estariam sujeito às regras e critérios próprios dos seus usos, endossa o direito da organização de monitorar as correspondências eletrônicas do empregado que a está representando através do "timbre" nome@empresa.com.br. Por outro lado há os que entendem que a lei do mundo real, o da inviolabilidade da correspondência, é aplicável no mundo virtual, vedando portanto qualquer tipo de monitoração.

Com as soluções RAS ou VPN ou tecnologias semelhantes de acesso remoto, o domínio das redes corporativa estão se estendendo para locais tão diversos e distantes como instalações de parceiros ou residência de empregados. O acesso nesses casos, apesar de feito através de equipamentos nem sempre de propriedade da empresa, deverá ser cercado de cuidados mínimos com relação à segurança. Deverão ter por exemplo a proteção de um antivírus de modo a não se tornar uma fonte de contaminação da rede corporativa e um Firewall "pessoal" para proteger contra os diversos tipos de ataque à rede utilizando a estação remota como ponte. Nesse último

caso, a estação remota mantém duas conexões: uma com a Internet estabelecida quando do acesso ao provedor por acesso discado ou por banda larga e a outra criada com o estabelecimento do túnel VPN; está portanto, criada mais uma abertura para um ataque que, iniciado no canal com a Internet, utiliza-se do túnel para que o invasor atinja a rede corporativa.

Considerando globalmente os aspectos de segurança, apesar de toda tecnologia disponível no mercado, a informação não estará protegida sem a participação correta de quem pode ser considerado o principal agente do processo, o usuário dos recursos de TI. É imprescindível a conscientização do importante papel que o mesmo desempenha e isso deve ser conseguido através da definição, divulgação e aceitação de uma política de segurança compatível com os processos da corporação, considerando o valor das informações que sejam importantes para o negócio.

Portanto, a tecnologia disponível devidamente implementada e utilizada é um dos componentes que juntamente com as políticas, procedimentos e principalmente o usuário, um ser humano, garantirão o nível de segurança desejado.

REFERÊNCIAS BIBLIOGRÁFICAS

Beal, Adriana – *"Esquemas de Falsificação de Informação: O Desafio de Proteger Conteúdo"*. Artigo publicado no Site da Módulo Segurity Solutions S.A., 25/Setembro/2002.

CSI/FBI - Pesquisa – *"2002 CSI/FBI Computer Crime and Security Survey"*, Vol VIII, No. 1, Spring 2002. Computer Security Institute e Federal Bureal of Investigations, 2002.

Leite, Celso H. – *"Vírus de Computador Inimigo Número um"*. Artigo publicado no Site da Módulo Segurity Solutions S.A., 01/Agosto/2001.

Maiwald, Eric; Sieglein, William – *Security Planning & Disaster Recovery.* Berkley: McGraw – Hill/Osborne, 2002.

Módulo - Pesquisa – *"Oitava Pesquisa Nacional sobre Segurança das Informações"*. Realizado pela Módulo Security Solutions S.A., 2002.

NAI - Artigo – *"An Introduction to Criptography"*. Network Associates Inc., 1999.

Nakamura, Emilio T.; Geus, Paulo L. – *Segurança em Redes.* São Paulo: Editora Berkley, 2002

Redes - Artigo – "*Backups*". Revista Redes, nº 2, Edição Agosto/2000. São Paulo: Editora Fittipaldi

RSA - Boletim – RSA Security Inc., 26/Setembro/2002.

Strebe, Matthews; Perkins, Charles – *Firewalls.* São Paulo: Makron Books, 2002

Symantec - Pesquisa – *"Primeira Pesquisa Symantec de Segurança de Sistemas de Informação"*. Symantec do Brasil, 15/Agosto/2002.