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

Oswaldo José Rodi Passerino

Esquemas de Segurança para Sistemas de Informação Baseados em Intranets

Orientador

Professor Vitório Bruno Mazzola, Dr.

Florianópolis, Junho de 2002.

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

Oswaldo José Rodi Passerino

Esquemas de Segurança para Sistemas de Informação Baseados em Intranets

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

Orientador

Professor Vitório Bruno Mazzola, Dr.

Florianópolis, Junho de 2002.

Esquemas de Segurança para Sistemas de Informação Baseados em Intranets

Oswaldo José Rodi Passerino

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

Prof. Dr. Fernando A. Ostuni Gauthier (Coordenador)

Banca Examinadora

Prof. Dr. Vitório Bruno Mazzola (Orientador)

Profª. Dra. Anita Maria da Rocha Fernandes

Prof. Dr. João Bosco da Mota Alves

AGRADECIMENTOS

Ao Professor e Orientador Vitório Bruno Mazzola, pela paciência, incentivo e dedicação durante a realização deste Mestrado.

Agradeço em especial a minha família, minha mãe Marlene pelo apoio e incentivo nas horas difíceis..., e pelo simples fato de ser minha mãe o qual tenho muito orgulho sem fim... ...Por meu pai Alphêo que me incentivou e aconselhou sempre que necessário... Minhas irmãs Maria José e Juliana que sempre estavam dispostas a me motivar e ajudar a me concentrar... e muito especialmente a minha Esposa Lucinéia Claudia pelo conforto, incentivo e apoio dados em todo o percurso desse meu caminho, em especial nos momentos em que pensava em desistir.

Aos amigos e colegas de serviço que estavam sempre dispostos a ajudar e participar com sugestões, conselhos e críticas.

A Universidade do Vale do Itajaí, Centro de Ciências Tecnológicas da Terra e do Mar, em particular, ao Curso de Ciência da Computação, pelo apoio e paciência expressados neste período.

SUMÁRIO

LISTA DE FIGURAS ix

LISTA DE TABELAS x

LISTA DE ABREVIATURAS xi

RESUMO xiv

ABSTRACT xv

CAPÍTULO I - INTRODUÇÃO 1

1. Introdução 1

2. Objetivos 2

2.1 Objetivo Geral 2

2.2 Objetivos Específicos 2

3. Organização do Trabalho 3

CAPÍTULO II - INTERNET 4

1. Histórico 4

1.1 ARPANET (Advanced Research Projects Agency Network) 6

1.2 NSFNET (National Science Foundation Network) 6

1.3 Surgimento da INTERNET 8

1.4 A INTERNET no Brasil 9

2. Serviços Disponibilizados na Internet 10

2.1 Acesso a Internet 10

2.2 Serviço de Correio eletrônico 11

2.2.1 Arquitetura e Serviços 12

2.2.2 Protocolos de Serviços 15

2.2.2.1 Protocolo de Transferência de Mensagens 16

2.2.2.2 Protocolos de Recebimento de Mensagens 17

2.3 Network News 18

2.4 Telnet 20

2.5 FTP 21

2.6 Gopher 22

2.7 *World Wide Web* 24

2.7.1 A Serviço do Lado do Servidor 25

2.7.2 O Serviço do Lado do Cliente 27

CAPÍTULO III - INTRANET 28

1. Conceituando uma Intranet 28

1.1 A World Wide Web e as Webs Internas 28

2. Intranets x Correio Eletrônico 29

3. As Intranets e o Groupware 30

4. Gerenciamento de Documentos em uma Intranet 31

5. O Funcionamento de uma Web Interna 32

5.1 TCP/IP: Uma Base de Rede de Baixo Custo 32

5.1.1 TCP/IP e o IETF 33

5.2 Endereçamento de Todos os Computadores 33

6. HTTP: Cliente/Servidor para o Restante do Pessoal 35

7. Motivos para se ter uma Intranet 37

CAPÍTULO IV – SEGURANÇA NA INTERNET 41

1. Introdução 41

2. Ameaças 42

3. Tipos de Ataques 45

3.1 Ataques técnicos 46

3.1.1 Ataques de Negação de Serviço 46

3.1.2 Ataques Furtivos 47

3.2 Ataques não Técnicos 49

4. Políticas de Segurança 50

5. Segurança do Correio Eletrônico 51

5.1 Ameaças a Mensagens em Trânsito 51

5.2 Ameaças aos agentes de entrega de mensagens em sistemas finais 52

6. Segurança dos Servidores de *News* 52

7. Segurança dos Servidores de Terminal 53

8. Protocolos de Segurança 54

8.1 IPSEC (*IP Security*) 54

8.2 SSL (Secure Sockes Layer) 56

8.3 PGP (Pretty Good Privacy) 56

8.4 PEM (Privacy Enhanced Mail) 57

8.5 SSH (Secure Shell) 58

8.6 HTTP Seguro 59

9. Criptografia 59

9.1 Criptografia com Chave Secreta 60

9.1.1 DES (Data Encryption Standard) 60

9.2 Criptografia com Chave Pública 63

9.2.1 RSA (Rivest, Shamir e Adleman) 63

10. Firewalls 65

10.1 Técnicas de *Firewall* 66

10.1.1 Filtros de Pacotes 67

10.1.2 Filtros "Inteligentes" 69

11. PROXY 70

11.1 Servidor *Proxy* de Aplicação 70

CAPÍTULO V – MODELO DE SEGURANÇA 72

1. Introdução **72**

2. Serviços a Disponibilizar **73**

2.1 Serviço de Autenticação **73**

2.1.1 A Escolha de uma Senha **73**

2.1.2 Mudança de Senha **74**

2.2 Serviço Web **74**

2.3 Serviço de DNS **75**

2.4 Serviço de FTP **76**

2.5 Serviço de Telnet **76**

2.6 Serviço de Correio Eletrônico **76**

2.6.1 Correio Eletrônico: O Alvo **77**

2.7 Serviço de Banco de Dados **78**

3. Tipos de Intranet **78**

3.1 Intranet Pura **79**

3.2 Intranet Intermediária **79**

3.3 Intranet E-Commerce **80**

4. Níveis de Segurança **81**

5. Como Proteger os Serviços? **82**

5.1 Serviço de Autenticação e Web **82**

5.2 Serviço de DNS **83**

5.4 Serviço de Correio Eletrônico **83**

5.5 Serviço de FTP **85**

5.6 Serviço de Banco de Dados **86**

6. Esquemas de Segurança **87**

CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES **91**

BIBLIOGRAFIA **93**

LISTA DE FIGURAS

Figura 1(a) Correio Postal. (b)Correio Eletrônico. (TANNENBAUM, 1997 – p738)... 15
Figura 2 Método de Criptografia DES (SOARES, 1995) 62
Figura 3 Intranet Pura 79
Figura 4 Internet Intermediária 80
Figura 5 Intranet E-Commerce 81
Figura 6 Esquema de Segurança de Intranet Pura 87
Figura 7 Esquema de Segurança Intranet Intermediária 89
Figura 8 Esquema de Segurança Intranet E-Commerce 90

LISTA DE TABELAS

Tabela 1 - Alguns URL's comuns 26
Tabela 2 - Classes de Ameaças (BERNSTEIN,1997 p. 29-30) 44
Tabela 3 - Algoritmos de Criptografia Simétricos (MAIA,2001) 63
Tabela 4 - Algoritmos de Criptografia Assimétrica (MAIA,2001) 65

LISTA DE ABREVIATURAS

AH	Header de Autenticação
API	*Aplication Program Interface*
ARPA	Advanced Research Projects Agency
ARPANET	*Advanced Research Projects Agency Network*
ASCII	*American Standard Code for Information Interchange*
CA	*Certification Authorities*
CCITT	*Comite Consultatif Internationale de Telegraphie et Telephonie*
CGI	*Common Gateway Interface*
CSNET	*The Computer Science Network*
DES	*Data Encryption Standard*
DHCP	*Domain Host Configuration Protocol*
DMSP	*Distributed Mail System Protocol*
DNS	*Domain Name System*
DoD	*Department of Defense*
ESP	*Dados de Segurança encapsulado*
FAPESP	Fundação de Amparo a Pesquisa do Estado de São Paulo
FTP	*File Transfer Protocol*
HTML	*Hiper Text Transfer Protocol*
HTTP	*Hyper Text Transfer Protocol*
IAB	*Internet Activities Board*

ICMP	*Internet Control Message Protocol*
IDEA	*International Data Encryption Algorithm*
IETF	*Internet Engineering Task Force*
IMAP	*Interactive Mail Access Protocol*
IMP	*Interface Message Processors*
IP	*Internet Protocol*
IPCA	*Internet Policy Certification Authorities*
IPSEC	*IP Security*
IPX	*Internetwork Packet eXchange*
LNCC	Laboratório Nacional de Computação Científica
MIT	*Massachussets Institute of Technology*
MOSS	*Mime Object Security Services*
MOTIS	*Messagerie Oriented Text Interchange*
MTA	*Mail Transport Agent*
NNTP	*Network News Transfer Protocol*
NPL	*Nuclear Physics Laboratory*
NSF	*National Science Foundation*
NSFNET	*National Science Foundation Network*
OSI	*Open Systems Interconnect.*
PCA	*Policy Certification Authorities*
PEM	*Privacy Enhanced Mail*
PGP	*Pretty Good Privacy*
POP	*Post Office Protocol*
RENPAC	Rede Nacional de Comutação por Pacotes
RNP	Rede Nacional de Pesquisa

RSA	*Rivest, Shamir and Adleman*
SHA	*Secure Hash*
SMTP	*Simple Mail Transfer Protocol*
SRI	*Stanford Research Institute*
SSH	*Secure Shell*
SSL	*Secure Sockes Layer*
TCP	Transmission Control Protocol
UA	*User Agent*
UCLA	*University of California at Los Angeles*
UCSB	*University of California at Santa Barbara*
UFRJ	*Universidade Federal do Rio de Janeiro*
URL	*Universal Rersource Location*
USENET	*Users' Network*
UUCP	*UNIX to UNIX Copy Program*
WWW	*World Wide Web*

RESUMO

Este trabalho foi desenvolvido visando um estudo das tecnologias de Internet e Intranet enfocando a vulnerabilidade de segurança existente. Após os estudos desenvolvidos, partiu-se para a definição dos perfis de intranet e os serviços a serem disponibilizados. Com o levantamento destes serviços verificou-se quais são suas vulnerabilidades e maneira de protegê-los. Após estes estudos elaborou-se o esquema de segurança para os diferentes perfis de Intranet.

ABSTRACT

This work was developed focus on a study of Internet and Intranet technologies about the security vulnerability. After the studies developed, the Intranet profiles definition and the services available started. With the survey of these services, was verified what are the vulnerability and the way to protect then. After the studies it was done the schema of security was done to different Intranet profiles.

CAPÍTULO I - INTRODUÇÃO

1. Introdução

Com a importação da tecnologia da Internet para o ambiente corporativo houve uma grande revolução dos negócios, de tal forma que a globalização está obrigando que as empresas procurem novos métodos para aumentarem sua eficiência e agilidade nos negócios. Isto trouxe a descoberta de que a rede privada de TCP/IP é tida como uma poderosa ferramenta de gestão administrativa e de disseminação de uma política cultural dentro da organização.

A informação tornou-se um elemento de fundamental importância e extremamente valiosa para os negócios de hoje. Devido a isto as empresas e instituições na maioria das vezes vêm cada vez mais utilizando recursos computacionais para armazenar, produzir e distribuir informações. Com isto da mesma maneira que vem aumentando a confiança das organizações em informações providas por sistemas computacionais, também vem ocorrendo um aumento quase que diário no surgimento de vulnerabilidades nos diversos sistemas disponíveis no mercado.

Uma Intranet quando não possui os controles de acesso apropriados, é um convite à rasura e à adulteração de documentos, de forma que a segurança de uma rede é considerada ao mesmo tempo, tanto uma questão tecnológica quanto política.

Como uma Intranet tem por finalidade a possibilidade de acesso imediato a informações corporativas, não quer dizer que qualquer pessoa possa acessar qualquer informação a qualquer momento. Para tal, os servidores Web das empresas não podem ser considerados simples ponto de acesso, como qualquer outro computador da empresa, pois assim trazem o aumento do risco para os dados.

Já que é extremamente insensato entrar na era da Intranet sem conhecimento tecnológico para entender os riscos e desprovido de regulamentação adequada para se formular uma política de segurança ideal com o intuito de definir procedimentos para proteger informações importantes da organização. Tornando assim a implantação de segurança em uma Intranet um processo difícil.

Para a implantação de segurança deve-se entender quais são as ameaças existentes e como reduzir a sua vulnerabilidade. Deve-se também ter consciência de quais são os recursos que desejam ser protegidos, que nível de segurança é mais adequado, dada à cultura e a filosofia da organização.

Para isto, é proposto o desenvolvimento de um esquema básico e de fácil entendimento para implantação da segurança em uma Intranet, de acordo com o seu tipo e abrangência, já que quando se fecha uma porta de acesso, os invasores acabam encontrando uma outra maneira, o que se torna impossível um sistema cem por cento intransponível.

2. Objetivos

2.1 Objetivo Geral

Este projeto tem por objetivo propor um esquema de segurança para Intranets nos seus diferentes tipos de perfis.

2.2 Objetivos Específicos

- Identificação de perfis de Intranets.

- Especificação dos serviços a disponibilizar (Banco de Dados, Servidor de Nomes, NAT, Comércio Eletrônico, etc. ...).

- Definição de níveis de segurança.

- Proposta de um esquema de segurança.

- Definição das funções de segurança no esquema.

3. Organização do Trabalho

O primeiro capítulo é este que está sendo apresentado.

O segundo capítulo traz uma apresentação sobre Internet, com suas principais características e funcionamento.

O terceiro capítulo trata das tecnologias da Intranet, sua utilização e motivos para seu uso.

O quarto capítulo trata da segurança na Internet, trazendo os tipos de problema, ataques e ameaças, apresentando também algumas soluções existentes.

O quinto capítulo trata dos métodos a serem utilizados de acordo com os níveis de segurança e o tipo da intranet, conforme as especificações deste mesmo capítulo.

O sexto capítulo traz as conclusões e considerações finais.

CAPÍTULO II - INTERNET

1. Histórico

No inicio da década de 1960, quando ocorria o auge da guerra fria, o DoD concebeu uma rede de controle que fosse capaz de sobreviver a uma guerra nuclear. Contudo as redes de telefonia e comutação de circuitos existentes eram tidas como muito vulneráveis, já que com a perda de uma linha ou comutação existiria o particionamento da comunicação, com isto a perda de comunicação entre as bases. Para que isto fosse resolvido o Pentágono convocou sua divisão científica, a ARPA - *Advanced Research Projects Agency*, para que esta resolvesse o problema (TANENBAUM, 1997).

Com um pequeno escritório e um orçamento reduzido para o padrão do Pentágono, a ARPA era responsável pela promoção de projetos de pesquisa de empresas e universidades que trabalhassem em prol das necessidades do Pentágono.

Os primeiros registros de que interações sociais poderiam vir a ser realizadas através das redes, datam de agosto de 1962. Este registros foram inúmeros memorandos escritos por J.C.R. Licklider, do MIT - *Massachussets Institute of Technology*, nos quais ele discutia o conceito de "Rede Galáxica". Nestes memorandos era previsto que vários computadores seriam interconectados globalmente, através desta interconexões todos poderiam acessar dados e programas de qualquer local rapidamente. Este conceito em sua essência tornou-se parecido com a Internet de hoje. Por Licklider ter sido o primeiro gerente do programa de pesquisa de computador do DARPA, ao iniciar seus serviços em outubro de 1962, consegui convencer seus sucessores Ivan Sutherland, Bob Taylor e Lawrence G. Roberts da importância do conceito de redes computadorizada.

O primeiro trabalho a ser publicado sobre a teoria de trocas de pacotes foi em julho de 1961, por Leonard Kleinrock do MIT. O primeiro livro que falava sobre o

assunto foi publicado em 1964. PEREIRA(2001) disse que quando Kleinrock conseguiu convencer Roberts da possibilidade teórica das comunicações usando pacotes ao invés de circuitos, deu um grande passo para tornar possíveis as redes de computadores. Outro fator que impulsionou foi o fato de conseguirem fazer os computadores conversarem entre si.

Roberts e Thomas Merrill conseguiram conectar um computador TX-2 em Massachussets com um Q-32 na Califórnia, no ano de 1965, por meio de uma linha discada de baixa velocidade, criando assim o primeiro computador em rede do mundo. Esta experiência foi bem sucedida no que diz respeito a capacidade dos computadores em trabalharem juntos, rodar programas e recuperar dados, contudo mostrou que o circuito do sistema telefônico era totalmente inadequado para o intento. PEREIRA(2001) disse que com isto confirmou-se assim a convicção de Kleinrock sobre a necessidade de trocas de pacotes.

Quando Roberts começou a trabalhar no DARPA, no final de 1966, no desenvolvimento do conceito das redes computadorizadas e elaborar o plano para a ARPANET, que foi publicado em 1967. Na mesma conferência onde ele apresentou este trabalho, também teve uma apresentação sobre o conceito de redes de pacotes desenvolvida pelos ingleses Donald Davies e Roger Scantlebury, da NPL-*Nuclear Physics Laboratory.*(Ibidem)

Em agosto de 1968, após Roberts e o grupo do DARPA refinaram as estruturas e especificações para a ARPANET, fez-se uma seleção para o desenvolvimento de um dos componentes-chave do projeto: o IMP - *Interface Message Processors*. Sendo selecionado um grupo dirigido por Frank Heart (*Bolt Beranek*) e Newman (BBN). Em paralelo ao trabalho do grupo da BBN nos IMPs com Bob Kahn assumindo um papel vital do desenho arquitetônico da ARPANET, PEREIRA(2001) afirma que o trabalho sobre a topologia e economia da rede estava sendo desenvolvido e otimizado por Roberts em conjunto com Howard Frank e seu grupo da *Network Analysis Corporation*,

enquanto o sistema de mensuração da rede estava sendo preparado pelo pessoal de Kleinrock na UCLA - *University of California at Los Angeles*.

1.1 ARPANET (Advanced Research Projects Agency Network)

No mês de dezembro de 1969, por serem os locais com um número grande de contratos com a ARPA e por terem computadores *hosts* com diferentes configurações e completamente incompatíveis, foram escolhidos UCLA, UCSB (*University of California at Santa Barbara*), SRI (*Stanford Research Institute*) e *University of Utah* como os quatros nós da rede experimental. Então conforme TANENBAUM(1997), após estes testes houve um aumento na produção e instalação de novos IMPs, fazendo com que a rede cresce-se rapidamente, de maneira que logo espalhou-se por todo o território norte americano.

MALAGRINO(1996) afirma que no início a ARPANET dava a possibilidade para a seus usuários de acesso através de um terminal remoto, de transferência de arquivos e de uso de impressoras e outros dispositivos remotos. No ano de 1971 a rede passou de 4 para 15 nós. Em 1972, já eram 37 nós. Contudo o acesso à rede era ainda era muito restrito, dando direito somente as instituições de pesquisa liga as ao governo e à área militar, tendo seu custo anual em cerca de US$ 250.000.

No ano de 1983 a ARPANET era tida como uma rede estável e bem-sucedida, e cada vez mais aumentava de tamanho. Porém no ano de 1990 a ARPANET foi desmantelada e desativada, sendo então substituída por redes mais novas.

1.2 NSFNET (National Science Foundation Network)

A NSF (*National Science Foundation*), no final da década de 1970, percebeu então o enorme impacto que a ARPANET estava causando sobre as pesquisas universitárias nos Estados Unidos, já que permitia aos cientistas do país inteiro

compartilharem dados e possibilitava que trabalhassem juntos em projetos de pesquisa. Porém, poucas universidades conseguiam se conectar a ARPANET, já que um dos requisitos necessário era possuir um contrato de pesquisa com o DoD, privilégio esse que muitas não tinham.A fim de resolver este problema a NSF configurou uma rede virtual, a CSNET, centralizada em uma maquina na BBN para oferecer linhas de discagem e conexões com a ARPANET e outras redes. TANENBAUM(1997) afirma que através da utilização da CSNET, os pesquisadores acadêmicos podiam estabelecer uma conexão e deixar uma mensagem de correio eletrônico para outras pessoas.

Quando iniciou, no ano de 1984, o desenvolvimento de uma rede de alta velocidade para suceder a ARPANET, a NSF quis abrir a rede para todos os grupos de pesquisas universitários. A partir da construção de uma rede de *backbones* para conectar as seis centrais de super-computadores da NSF, em *San Diego*, *Boulder*, *Champaign*, *Pittsburgh*, *Ithaca* e *Princeton*. Os supercomputadores de acordo com TANENBAUM(1997), receberam um micro-computador LSI-11 denominado *fuzzball*, que por sua vez eram conectados a linhas privadas de 56 Kbps, formando assim a sub-rede, que estava utilizando a mesma tecnologia de hardware da ARPANET.

Quando Dennis Jennings, no ano de 1985 começou a liderar na NSF o programa da NSFNET, com o auxilio da comunidade ajudou a NSF a tomar uma decisão crítica: que TCP/IP iria ser mandatório para o programa da NSFNET. Já no ano de 1986 quando Steve Wolff juntou-se a NSFNET, reconheceu a necessidade de uma infraestrutura de rede maior para dar suporte as comunidades acadêmicas e de pesquisa, além é claro da necessidade do desenvolvimento de uma estratégia para estabelecer esta infra-estrutura independentemente dos recursos federais. PEREIRA(2001) afirma que então políticas e estratégias foram adotadas para atingir este fim.

A NSF decidiu suportar a infra-estrutura organizacional da Internet da DARPA já existente, que era hierarquicamente arranjada pelo então *Internet Activities Board* (IAB). Para PEREIRA(2001) com a declaração pública desta opção feita em conjunto pelo grupo de Engenharia e Arquitetura da Internet da IAB e pelo grupo de Assessoria

Técnica de Rede da NSF do RFC 985 - *Requirements for Internet Gateways,* assegurando formalmente a interoperabilidade entre DARPA e NSF.

A comunicação entre a ARPANET e a NSFNET foi diretamente através do TCP/IP, já que ambas possuíam softwares diferentes. Criando assim de acordo com TANENBAUM(1997) a primeira WAN TCP/IP. A criação da NSFNET foi um sucesso instantâneo, passando a funcionar com sua capacidade máxima em pouco tempo. De imediato a NSF começou a planejar seu sucessor e, para administra-lo, contratou o consorcio MERIT, de *Michigan*.

Os anos se passaram e outros países e regiões do mundo construíram suas redes comparáveis a NSFNET, como o EBONE e a EuropaNET, e cada país possuía uma rede do porte das redes regionais da NSF.

1.3 Surgimento da INTERNET

Com o aumento do número de redes, máquinas e usuários conectados na ARPANET após o TCP/IP torna-se o único protocolo oficial, em 1° de Janeiro de 1983. E quando a NSFNET e a ARPANET foram inter-conectadas, este crescimento tornou-se exponencial. Muitas redes regionais foram integradas e criadas conexões com redes no Canadá, Europa e Pacífico (TANENBAUM, 1997)

A denominação de INTERNET para esta rede teve início em meados da década de 80, pois as pessoas começaram a considerar os conjuntos de rede como uma inter-rede. Seu crescimento continuou acelerado e no ano de 1990 já interconectava 3 mil redes e 200 mil computadores. No ano de 1992, foi conectado o milionésimo *host*.

Quando no ano de 1990 os interesse militares da ARPANET foram transferido para a MILNET, MALAGRINO(1996) que com isto a ARPANET foi então definitivamente extinta. Enquanto isso ocorria, a Internet continuava crescendo, abrindo

espaço para usuários comerciais, fora da esfera acadêmica, que demandavam por serviços de utilização mais simples.

A partir do ano de 1993, a Internet deixou de ser uma instituição de natureza apenas acadêmica e passou a ser explorada comercialmente, para tal foram construídos novos *backbones* por empresas privadas (PSI, UUNet, Sprint etc.) quanto para fornecimento de serviços diversos. Abrindo-se assim, em nível mundial.

1.4 A INTERNET no Brasil

A Internet chegou ao Brasil em 1988 pela iniciativa da comunidade acadêmica de São Paulo através da FAPESP — Fundação de Amparo a Pesquisa do Estado de São Paulo, e do Rio de Janeiro UFRJ — Universidade Federal do Rio de Janeiro e LNCC — Laboratório Nacional de Computação Cientifica.

O Ministério da Ciência e Tecnologia criou no ano de 1989, a Rede Nacional de Pesquisa (RNP), que é considerada uma instituição que tem por objetivo iniciar e coordenar a disponibilizarão de serviços de acesso a Internet no Brasil, partiu-se da criação do *backbone* da RNP, que interligava as instituições educacionais a Internet.

Conforme SOUZA(1999), “a exploração comercial da Internet iniciou-se em dezembro de 1994, a partir de um projeto-piloto da Embratel...”, este projeto permitia inicialmente o acesso a Internet através de linhas telefônicas discadas, mais tarde, através de acessos dedicados via RENPAC ou linhas E1 (categoria de velocidade).

A ampliação do *backbone* RNP no que se refere à velocidade e numero de POPs, a fim de suportar o trafego comercial de futuras redes conectadas aos POPs, foi uma das etapas do processo de implantação da Internet comercial. Segundo SOUZA (1999) “esse *backbone* a partir de então passou a se chamar Internet/Br”.

2. Serviços Disponibilizados na Internet

2.1 Acesso a Internet

De acordo com SOUZA (1999), o acesso a Internet é feito através de provedores de acesso. Aonde o usuário conecta-se de casa, por exemplo, através de uma ligação telefônica entrem o modem do usuário e o modem do Provedor. Este provedor possui diversos *modens* para que possa atender a todas as ligações a serem conectadas a um servidor, que transforma esta ligação em um acesso a Internet.

Os provedores de acesso também podem hospedar as *home-pages* de seus clientes, para que estas sejam acessadas pelo mundo todo. O acesso a um provedor faz-se através de um LOGIN e uma SENHA.

O acesso de um computador à Internet refere-se à execução de aplicações relacionadas a essa rede, podendo ser classificado em:

- **Acesso Completo:** este tipo de acesso ocorre quando existe um computador que tenha um software TCP/IP que possa ser endereçável na Internet, de forma que possa executar aplicações que interajam diretamente com aplicações de outros computadores da Internet, sendo desta maneira um *host* da Internet (CARVALHO, 1998).

- **Acesso Limitado:** este tipo de acesso ocorre quando o computador não possui um software TCP/IP, possui apenas acesso a um computador "*host*" que possua acesso complete a Internet, de maneira que se torna um acesso indireto, sendo assim ele não é um *host* da Internet. (CARVALHO, 1998).

Existe também outra classificação quanto à forma de conexão a um provedor e acesso, e o seu ponto de acesso à Internet, sendo elas:

- **Conexão Permanente:** ocorre quando a ligação entre o computador em questão e a Internet é estabelecida através de circuitos dedicados de comunicação. Utilizada normalmente por computadores que possuam acesso completo a Internet, endereço e nome de domínio fixo, sendo assim localizáveis por qualquer outro computador da rede. (CARVALHO,1998)

- **Conexão Temporária:** esta forma de conexão ocorre tanto com computadores que possuam acesso completo quanto aos com acesso limitado a Internet, ocorrem normalmente através de linhas telefônicas discadas quando existe o estabelecimento da ligação entre os dois computadores, o cliente e servidor (CARVALHO, 1998).

2.2 Serviço de Correio eletrônico

Os correios eletrônicos são serviços que permitem a troca de mensagens entre usuários através da Internet e os de maior alcance, já que permitem a troca de mensagens tanto com usuários de outras redes de serviços, quanto com usuários de redes corporativas não totalmente interligadas à Internet.

Os primeiros sistemas de correio eletrônico existentes, segundo TANENBAUM (1997), eram simplesmente formados por protocolos de transferência de arquivos. Estes possuíam a convenção de que a primeira linha de cada mensagem deveria conter o endereço do destinatário.

Com o passar do tempo quanto mais as pessoas ganham experiência, projetavam sistemas de correio eletrônico mais elaborados. Até que em 1982, as novas propostas de sistemas de correio eletrônico da ARPANET foram publicadas como a RFC 821 (protocolo de transmissão) e a RFC 822 (formato de mensagem). Após dois anos de acordo com TANENBAUM (1997) o CCITT esboçou sua recomendação X.400, que mais tarde foi considerada como base para o MOTIS do modelo OSI. Contudo após

uma década de concorrência, os sistemas de correios eletrônicos baseados na RFC 822 passaram a ser amplamente usados, ao passo de que aqueles baseados na X.400 desapareceram no horizonte.

O Correio eletrônico possui como base o endereço eletrônico ou mais conhecido como "*e-mail address*". Conforme CARVALHO (1998) este endereço possui o seguinte formato padrão: **usuário@host** .

- **Usuário:** é o identificador de uma caixa postal na qual será recebida a mensagem;

- ***Host*:** é o domínio do equipamento aonde se encontra a caixa postal.

Para TANENBAUM (1997) e CARVALHO (1998), o funcionamento do correio eletrônico baseia-se no paradigma '*store-and-forward*' no qual os usuários envolvidos na transferência de uma mensagem não interagem diretamente si, mas sim através de programas servidores encarregados de executar e gerencia esta transferência.

2.2.1 Arquitetura e Serviços

Os componentes principais que formam um sistema de correio eletrônico de acordo com CARVALHO (1998) são:

- ***User Agent* (UA):** é o software que interage com o usuário, sendo responsável em obter as mensagens a serem enviadas, e buscar as mensagens recebidas;

- ***Mail Transport Agent* (MTA):** é o software que possui a responsabilidade de transportar as mensagens entre os envolvidos, através da Internet.

- ***Mail Boxes*:** são as caixas postais para armazenamento das mensagens recebidas

Conforme TANENBAUM (1997) os correios eletrônicos desempenham cinco funções básicas, sendo elas:

1. **Composição:** processo referente à criação de mensagens e respostas. Pode ser utilizado qualquer tipo de editor para o corpo da mensagem, e o sistema auxilia com o endereçamento e com os inúmeros campos de cabeçalho anexado em cada mensagem.

2. **Transferência:** processo referente ao deslocamento de uma mensagem entre o remetente e o destinatário. Este processo necessita do estabelecimento de uma conexão com o destino ou com alguma máquina intermediária. O sistema de correio eletrônico pode fazer isso automaticamente, sem perturbar o usuário.

3. **Geração de Relatório:** processo utilizado para informar ao remetente sobre o que aconteceu com a mensagem. Existem inúmeras aplicações em que a confirmação da entrega da mensagem é importante e pode ter até mesmo uma significância legal.

4. **Exibição das Mensagens:** processo necessário para que as pessoas possam ler suas mensagens de correio eletrônico. Ás vezes são necessárias conversões ou deve-se acionar algum visualizador especial.

5. **Disposição:** considerada a última etapa, refere-se ao que o destinatário faz com a mensagem depois de recebê-la.

Hoje em dia os sistemas de correio eletrônico são largamente usados para comunicação em uma empresa, já que permite com que funcionários fisicamente distantes interajam e cooperem em projetos de grande complexidade. Com isto os correios eletrônicos eliminam a maior parte dos assuntos relacionados a classes sociais, faixas etárias e sexo, e os debates via correio eletrônico tendem a se concentrar em idéias, e não nas situações das empresas.

De acordo com TANENBAUM (1997),

> *"Uma idéia chave em todos os sistemas de correio eletrônico é a distinção entre o envelope e seu conteúdo. O envelope encapsula a mensagem. Ele contém todas as informações necessárias para o transporte da mensagem, como o endereço de destino, a prioridade e o nível de segurança, sendo todas elas distintas da mensagem em si. Os agentes de transportes da mensagem utilizam o envelope para entregá-lo, exatamente como uma agência de correio".*

Uma mensagem dentro do envelope é composta por duas partes: o cabeçalho onde estão contidas as informações de controle a serem utilizadas pelos agentes, e o corpo da mensagem que se destina inteiramente a seu destinatário. Como na Figura1.

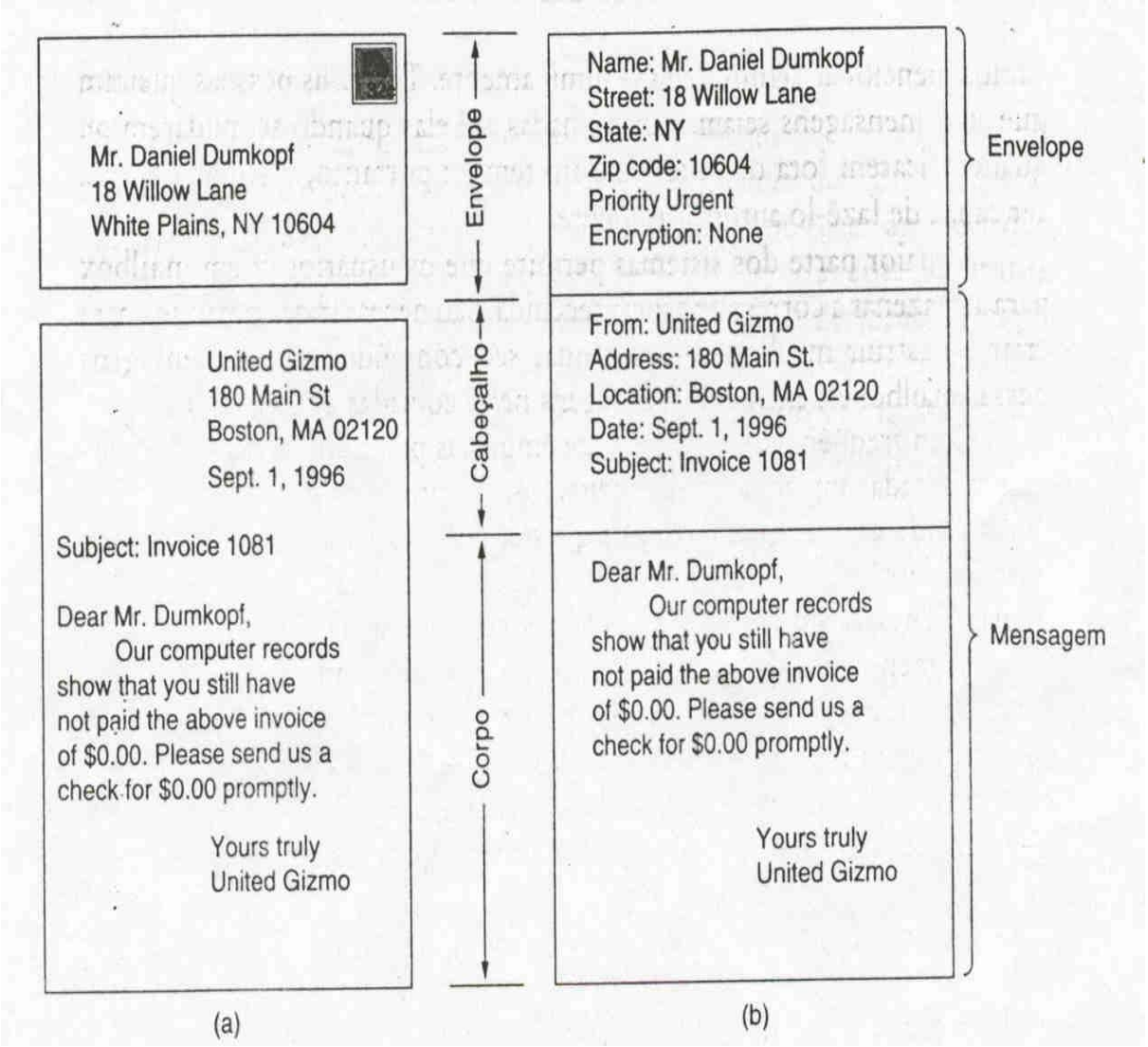


Figura 1(a) Correio Postal. (b)Correio Eletrônico. (TANNENBAUM, 1997 – p738)

2.2.2 Protocolos de Serviços

De acordo com TANENBAUM (1997) o serviço de correio eletrônico utiliza os protocolos SMTP (*Simple Mail Transfer Protocol*) para o envio de mensagens, e um dos seguintes protocolos para recebimento de mensagens: POP3 (*Post Office Protocol*), **IMAP** (*Interactive Mail Access Protocol*) ou DMSP (*Distributed Mail System Protocol*).

2.2.2.1 Protocolo de Transferência de Mensagens

Para que as mensagens de correio eletrônico sejam entregues é necessário que a máquina de origem faça uma conexão TCP com a máquina destino através da porta 25 da máquina de destino. Para que isto ocorra existe um processo que fica escutando a porta SMTP (*Simple Mail Transfer Protocol*) a procura de requisições de envio de correios eletrônicos. Quando a conexão é estabelecida este processo recebe e copia as mensagens que estejam contidas nela, transferindo as para as *mailboxes* apropriadas. Caso esta mensagem não possa ser entregue, TANENBAUM (1997) diz que o sistema deverá gerar um relatório de erros contendo a primeira parte da mensagem não entregue será retornada ao remetente.

Quando a entrega de mensagens for local, envolve mais aspecto que somente anexar a mensagem que chega à caixa postal do destinatário. Em geral o MTA local irá executar tarefas relacionadas com o uso de nomes alternativos ou apelidos e também o reenvio de mensagens. Também existem para MORAES NETO (1999) as mensagens que não poderão ser entregues e que serão devolvidas, ou seja, retornadas para o remetente com alguma mensagem de erro.

O SMTP é considerado um protocolo muito simples por ser ASCII.O funcionamento dele ocorre após a máquina de transmissão estabelecer a conexão TCP com a porta 25 operando como cliente, espera que a máquina de recepção opere como servidor, comunique-se primeiro. Então o servidor começa por enviar uma linha de texto informando sua identidade e indicando se está ou não preparado para receber mensagem. Caso não esteja, o cliente encerrará a conexão e tentará outra vez mais tarde.

Quando o servidor está querendo receber mensagens, o cliente então anuncia de quem veio a mensagem e a quem se destina. Caso exista o destinatário no servido local do destino, o servidor então sinaliza ao cliente que este já pode enviar a mensagem. Logo em seguida, o cliente enviará a mensagem e o servidor vai confirmá-la. O TCP fornece um fluxo de *bytes* confiável, tornando-se desnecessário a soma de verificações

de envio de mensagens. TANNENBAUM (1997) afirma que se houverem mais mensagens elas serão enviadas, até que não exista mais nenhuma e a conexão possa ser encerrada.

Quando o envio de mensagens ocorre em redes UUCP, estas não serão normalmente entregues diretamente, mas sim reenviadas para a máquina de destino através de um conjunto de sistemas intermediários. Quando necessita enviar uma mensagem através de uma conexão UUCP, o MTA remetente em geral executará o programa *rmail* no sistema que fará o reenvio, usando o programa *uux* e escrevendo a mensagem na entrada padrão do sistema remoto.(MORAES NETO, 1999)

Como isto é feito para cada mensagem separadamente, existe a possibilidade de se produzir uma considerável demanda nos principais pontos de reenvio de mensagens, assim como seria possível congestionar as filas de tarefas temporárias do UUCP com milhões de mensagens utilizando uma quantidade de disco descomunal.

2.2.2.2 Protocolos de Recebimento de Mensagens

Os correios eletrônicos utilizam protocolos específicos para o recebimento das mensagens por seus usuários. De acordo com TANENBAUM (1997) o protocolo mais simples a ser utilizado para o recebimento de mensagens contidas em um *mailbox* remota é o POP3 (*Post Office Protocol*), este protocolo foi definido na RFC 1225. é um protocolo baseado em comandos nos quais os usuários podem estabelecer *logins* e *logouts*, e comandos para obter e eliminar mensagens. O POP3 consiste em um texto ASCII semelhante ao SMTP, que tem por objetivo obter as mensagens de *mailbox* remotas e, após, armazená-las na máquina local do usuário para leitura futura.

Existe também um protocolo mais sofisticado para entrega de mensagens, sendo este o IMAP (*Interactive Mail Access Protocol*), que é definido na RFC 1064. Este protocolo foi projetado para auxiliar o usuário que utiliza diversos computadores.Possui

como idéia que o servidor de correio eletrônico mantenha um repositório central que possa ser acessado a partir de qualquer máquina pelo usuário.

Outro protocolo existente para o recebimento de mensagens é o DMSP (*Distributed Mail System Protocol*), o qual faz parte do sistema PCMAIL e é descrito na RFC 1056. Esse protocolo não presume que todas as mensagens estejam em um servidor, como acontece com o POP3 e o IMAP. Este protocolo permite aos usuários fazer um *download* de suas mensagens do servidor para uma estação de trabalho, PC ou laptop e, em seguida, desconectar-se. Estas mensagens poderão ser lidas e respondidas enquanto não houver conexão. TANNENBAUM (1997) diz que quando a reconexão ocorrer mais tarde, as mensagens serão transferidas e o sistema será ressincronizado.

2.3 Network News

O serviço de *Network News* (*Usenet News* ou *News*) conforme CARVALHO (1998) é composto por informações agrupadas por categorias e programas responsáveis pelo seu intercambio, divulgação e acesso. Este tipo de serviço originou-se a partir dos usuários da rede USENET (era uma rede acadêmica de equipamentos com Sistema Operacional UNIX conectados através de linhas telefônicas discadas via UUCP). Está amplamente difundido pela Internet nos dias de hoje.

As informações ou assuntos são divididos em categorias de acordo com as áreas de interesse, estes agrupamentos são denominados de *NEWSGROUPS* (Grupos de Notícias). Sua organização é feita de forma hierárquica, eles partem de um tipo de atividade até o assunto propriamente dito. De acordo com CARVALHO (1998) existe uma divisão destes grupos em dois tipos: livres (quando não ha controle sobre as informações envolvidas) ou moderados (quando ha uma triagem dessas informações antes da sua publicação).

O *newsgroup* é composto por uma unidade denominado artigo, que possui o formato bem semelhante ao das mensagens do sistema de correio eletrônico. Assim sendo, o serviço *NetNews* permite aos usuários, selecionar um ou mais grupos de seu interesse, podendo fazer desde a simples leitura de artigos até o envio de artigos próprios ou respostas a outros artigos.

O serviço de *News* funciona através do envio de um artigo para um determinado endereço, e este é distribuído para programas-servidores espalhados pela Internet conhecidos como *News Servers*, de acesso público ou não, que trabalham em colaboração entre si (*Newsfeed*). Após isto, os usuários para terem acesso a esses artigos necessitam de um programa cliente denominado de *News Reader*.(CARVALHO, 1998)

O programa *News* Reader é responsável tanto a subscrição de um usuário a um grupo quanto o controle dos artigos lidos. Desta forma o servidor ao qual o usuário possui permissão de acesso apenas disponibiliza os artigos pertinentes aos grupos de interesse de sua comunidade de usuários. Para que sejam ágeis os servidores a disponibilização dos artigos é temporária, isto é, os artigos possuem uma data de expiração.

A forma de envio de artigos conforme CARVALHO (1998) para um dado grupo (*news posting*) é feito normalmente da mesma maneira com que é enviada uma correspondência a uma lista de discussão de correio eletrônico, desta forma então existem determinados programas responsáveis por executar a transferência de um artigo de uma lista de discussão para um *newsgroup* (*mail-to-news gateways*)

Com o avanço da Internet, o protocolo *news* passou a permitir que um usuário da Web chame um artigo de *newsgroup* como se fosse uma página da Web. Tornando assim, um *browser* também um *newsreader*. Devido a isto, muitos *browsers* possuem botões ou itens de menu para tornar a leitura de artigos USENET ainda mais fácil do que quando se usa os *newsreaders* padrão.

O protocolo *news* aceita somente dois formatos:

1. o primeiro especifica um *newsgroup* e pode ser usado para obter uma lista dos artigos de um site de artigos pré-configurado.

2. o segundo exige que seja fornecido o identificador de um artigo de *newsgroup* específico. O *browser* busca então o artigo em seu *site* de artigos pré-configurado, usando o protocolo NNTP.

2.4 Telnet

As aplicações baseadas no serviço de *Telnet* permitem que usuários remotos acessem computadores *host* com TCP/IP como se fosse um terminal do mesmo, executando programas e comandos residentes no *host*. Por isso CARVALHO (1998) afirma que estes equipamentos remotos devem ter um sistema Operacional multitarefa do tipo UNIX ou OS/2 por exemplo, e que possuam mecanismos de autorização de acesso via sistema de contas e autenticação (*login* ou *logon*). Por isto classifica-se o serviço *Telnet* de um serviço de *login* remoto da Internet.

O usuário para interagir com o serviço *Telnet* necessita de um programa-cliente *Telnet*, selecionando o equipamento onde deseja executar uma dada aplicação ou programa. Para MARQUES (1995) em primeiro lugar o usuário deverá saber o nome do computador ou *Host* que deseja acessar. O servidor que possui o serviço de *telnet* enviará um *prompt* para que seja estabelecida a sessão, normalmente este *prompt* irá solicitar uma identificação do usuário e também uma senha. A identificação do usuário é considera como uma conta de usuário, *user-id*, *username*, *login*, servido para que a estação em que ele se encontra possa ser autorizada a utilizar os serviço no servidor. Já a senha, também chamada de *password*, prova que é realmente o usuário que está solicitando acesso.

No caso do computador que está sendo acessado não forneça um sistema de menu de navegação, o usuário pode utilizar os comandos nativos do servidor para executar o que deseja.

Para MARQUES (1995) os novos usuários do *Telnet* enfrentam um grande problema para fazer o encerramento da sessão que foi aberta. Este problema possui uma solução simples e fácil, basta prestar atenção na hora em que se está fazendo uma conexão *Telnet*, pois o servido em geral dá dicas de como proceder com o encerramento da sessão. Caso nada seja dito, deve-se tentar os seguintes comandos: *exit, quit, logout, logoff, stop, bye, goodbye, leave, disconnect*, fim, x (maiúsculo ou minúsculo), q (maiúsculo ou minúsculo), CTRL-D, CTRL-Z.

2.5 FTP

O FTP (*File Transfer Protocol*) é o serviço da Internet que oferece a possibilidade de transferência de arquivos. Este é um dos serviços mais utilizados na Internet, sendo responsável por quase 70% do tráfego de dados na rede.

A transferência de arquivos é a possibilidade que os usuários podem obter ou enviar artigos de uma máquina para outra ligada a Internet. Para que isto aconteça CARVALHO (1998) diz que o FTP baseia-se no estabelecimento de uma sessão limitada entre o cliente local e o servidor. Possui uma autenticação semelhante ao *Telnet*, contudo possui somente comandos que se relacionem com manipulação de diretórios, conseguindo assim o usuário pesquisar a estrutura de diretórios e arquivos do servidor, para então selecionar algum arquivo e efetuar a transferência.

O servidor de FTP para ser acessado por um usuário que não possua uma conta nele, disponibiliza uma conta especial denominada de *anonymous* e com autenticação flexível, em geral um endereço de e-mail Após o estabelecimento da sessão o usuário

possui acesso apenas aos arquivos que podem ser consultados ou transferidos para seu computador.

Este serviço de FTP é utilizado em grande escala na Internet, de tal forma que TANENBAUM (1997) afirma que com "a Web não muda isso, ela apenas torna a obtenção de arquivos via FTP mais fácil, pois o FTP tem uma interface um tanto misteriosa." O FTP via Web ocorre através do protocolo HTTP, não sendo necessário a existência do serviço de FTP na máquina. Com isto esta cada vez mais sendo desativados servidores de FTP puro para serem utilizados via HTTP, pois traz mais benefícios além dos disponibilizados pelo FTP.

Conforme SOUZA (1999), "os arquivos transferidos na Internet podem ter vários formatos como imagem, texto e binário". Alguns destes arquivos podem ser visualizados com a utilização de um *browser*, outros, porém, necessitam de *softwares* especiais para visualização.

O processo de puxar e copiar um arquivo da Internet é denominado de *download*, e de acordo com SOUZA (1999) os arquivos para *download* em geral já são disponibilizados automaticamente pelo FTP nas paginas Web pelo *browser* de acesso. Assim sendo pode-se copiar um arquivo de dados ou programa de algum servidor da Internet para o disco do computador local.

2.6 Gopher

No ano de 1991 a universidade de Minnesota (EUA) desenvolveu um sistema de procura e transferência de informações orientadas a títulos de documentos, este serviço passou a ser denominado *Gopher*, que segundo CARVALHO (1998) permite que um usuário localize uma certa informação (texto, imagem, multimídia etc.), na Internet sem que seja necessário conhecer a exata localização da mesma.

De acordo com TANENBAUM (1997) o *Gopher* foi "batizado com o nome dos times de atletas daquela escola, os *Golden Gophers* (e que também é uma gíria que significa "go for", ou seja, vá buscar). O *Golphers* é muitos anos mais velho do que a *Web*."

No *Gopher* as informações estão disponibilizadas para os usuários através da utilização de programas servidores que possuem menus com itens que podem estar associados a arquivos de informações, outros itens de menu, ou mesmo programas a serem executados. Devido a essa estrutura temos como resultado uma arvore de menus, da forme que cada item de um menu possui um descritor que indica o tipo e o equipamento da Internet onde reside.

Esta árvore de menus de acordo com CARVALHO (1998) é utilizada para a navegação do usuário através de um cliente *Gopher* do tipo "*information browser*", o qual interage com o servidor *Gopher* primeiramente escolhido pelo usuário, que fornece um menu-raiz, par a partir daí o usuário dar inicio a sua navegação. Sendo assim considerado com um mecanismo semelhante a Web para a recuperação de informações, contudo não aceita imagens, somente textos.

> *"A grande vantagem do Gopher sobre a Web é que ele funciona bem em terminais ASCII de 25 X 80, que ainda existem por aí e, por funcionarem no modo de texto, são muito rápidos,. Por isso, há milhares de servidores Gopher no mundo. Ao usar um protocolo gopher, os usuários da Web podem acessar servidores Gopher e ter seus menus apresentados como um página da Web."*(TANNEMBAUM, 1997)

2.7 *World Wide Web*

A partir do ano de 1989 Laboratório de Pesquisas Nucleares – CERN – em Genebra na Suíça desenvolveu a *World Wide WEB – WWW* (Teia de Alcance Mundial) para que fossem interligados os pesquisadores de inúmeros institutos através da Internet, de tal forma que CARVALHO (1998) afirma que "esse é sem duvida, o sistema cuja utilização mais cresce atualmente na Internet, sendo o maior responsável pelo aumento dessa rede nos últimos anos."

Seu primeiro módulo a estar em funcionamento em um ano e meio depois foi o protótipo que funcionava em modelo texto, sendo demonstrado publicamente em dezembro de 1991 na conferência *Hypertext* '91, em *San Antônio* no *Texas.* Após esta demonstração, TANENBAUM (1997) afirma que "seu desenvolvimento prosseguiu no ano seguinte e culminou com o lançamento da primeira interface gráfica, o Mosaic, em fevereiro de 1993..."

Por ser um sistema de busca e obtenção de informações embutidas nos documentos e não no titulo dos documentos, a WWW sendo então diferente do *Gopher*. Este tipo de procura é conhecido como navegação por hipertexto. Por se diferente, a WWW não cria como no *Gopher* uma imagem de uma árvore, mais sim a imagem de uma teia que interliga documentos através da Internet — dai o seu nome *World Wide Web*, ou seja, Teia de Alcance Mundial.

Os documentos que compõem a Web contém na sua grande maioria imagens e recursos de multimídia, sendo então denominados de documentos hipermídia. A criação destes documentos é feita a través da linguagem de programação HTML (*Hiper Text Markup Language*), baseada nas diretivas do formato ASCII, permitindo assim a definição do formato do documento e as ligações com os outros documentos, e como CARVALHO (1998) disse, estes documentos podem estar em outros *sites*, passando então a ser denominada de *hyperlink*.

2.7.1 A Serviço do Lado do Servidor

O funcionamento de um Servidor WWW é através de processos que estão rodando e escutando na porta 80 TCP, no aguarde da solicitação de conexão de um cliente. TANENBAUM (1997), diz que após o estabelecimento desta conexão o cliente envia uma solicitação ao servidor e este envia uma resposta. Após este processo a conexão é liberada. Contudo para que ocorra estas solicitações e repostas é necessário a utilização do protocolo HTTP (*HyperText Transfer Protocol*), o qual valida todas estas interações.

Conforme TANENBAUM (1997), "cada interação consiste em uma solicitação ASCII, seguida de uma resposta RFC 822 do tipo fornecido pelo MIME. Embora o uso do TCP para a conexão de transporte seja bem comum, essa não é uma exigência formal de padrão".

Existem cada vez mais versões do HTTP, pois este está sempre em evolução, de tal forma que, em quando inúmeras versões estão sendo utilizadas, outras estão em desenvolvimento. Este protocolo consiste de acordo com TANENBAUM (1997) de dois itens razoavelmente distintos: um conjunto de solicitações dos *browsers* aos servidores e um conjunto de respostas que retornam no caminho inverso.

Apesar das inúmeras versões do HTTP, todas aceitam como padrão dois tipos de solicitação:

- Simples: é apenas uma linha GET que identifica a página desejada, sem ter a versão do protocolo. Possuindo como resposta uma página sem cabeçalho, sem MIME e sem protocolo.

- Completa: é uma linha GET que identifica a página desejada, possuindo a versão do protocolo. Possuindo como resposta uma página com cabeçalho, com MIME e com protocolo.

Para que os documentos HTML ou outro tipo de informação seja encontrada na Web foi criado de acordo com CARVALHO (1998) um identificador denominado de URL(*Universal Resource Location*).

Este identificador é atribuído a cada página como um nome universal para ela. Sendo dividido em três partes conforme TANNENBAUM (1997):

- O Protocolo;
- O nome DNS da máquina que hospeda a página;
- E o nome da página (em geral um nome de arquivo).

Para se acessar páginas na Web foram definidos outros protocolos e URL's conforme a Tabela 1.

Nome	**Usado para**	**Exemplo**
HTTP	Hypertext (HTML)	http://www.cbcomp.univali.br
FTP	FTP	ftp://ftp.inf.univali.br/pub
File	Arquivo Local	/usr/Cbcomp/programa.c
News	*Newsgroup*	news:cbcomp.os.minix
News	Artigo de *Newsgroup*	news:AAO12354312@cbcomp.univali.br
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Enviar Mensagem	mailto:cbcomp@cbcomp.univali.br
telnet	Login remoto	telnet:/www.cbcomp.univali.br

Tabela 1 - Alguns URL's comuns

Os servidores de WWW não possuem somente os serviços de navegação, podem também implementar interfaces com quaisquer outros serviços disponíveis em equipamentos da Internet. CARVALHO (1998) afirma que para oferecer tais serviços é necessária a utilização de uma interface conhecida como CGI (*Commom Gateway Interface*), de forma que estes servidores possam interagir com qualquer programa ou serviço disponível através de programas ou sistemas conhecidos como *gateways* para WWW. Estes *gateways* são comumente utilizados para autorizarem a interação dos usuários com programas que permitam o preenchimento de formulários, de forma que possibilitem um número amplo de serviços, desde transações comerciais até pesquisas em bases de dados.

2.7.2 O Serviço do Lado do Cliente

O serviço de WWW pelo lado do cliente é feito através de um programa denominado de *browser* ou navegador WWW, utilizado para a obtenção de um documento HTML ou outro tipo de informação. Seu funcionamento é através da interação com o servidor WWW do equipamento que possua uma informação a ser enviada via protocolo HTTP, e conforme CARVALHO (1998), este cliente é responsável pela interpretação e visualização das informações.

CARVALHO (1998) afirma também que "os navegadores (*browsers*) WWW normalmente interagem também com outros servidores de informações (*Gopher*, FTP), obtendo deles informações e as apresentando como se fossem documentos hipertexto".

CAPÍTULO III - INTRANET

1. Conceituando uma Intranet

O que é uma Intranet?

BENETT (1997) responde a esta pergunta da seguinte maneira:

> *"O termo "intranet" começou a ser usado em meados de 1995 por fornecedores de produtos de rede para se referirem ao uso dentro das empresas privadas de tecnologias projetadas para a comunicação por computador entre empresas. Em outras palavras, uma intranet consiste em uma rede privativa de computadores que se baseia nos padrões de comunicação de dados da internet pública."*

Ou seja, uma Intranet do ponto de vista das empresas, seria um meio privativo que possibilita a troca de informações e oferecendo vantagens inigualáveis em termos de custo e recursos através da integração de serviços de redes tradicionais.

1.1 A World Wide Web e as Webs Internas

As *Webs* Internas são diferenciadas da WWW não pela tecnologia utilizada, mais sim para o uso que se pretende fazer delas. O crescimento das *Webs* Internas é cada vez mais rápido, pois conforme BENETT (1997) disse dentre dos limites empresariais a maioria dos problemas relacionados ao comércio eletrônico simplesmente não existem, de forma que não dificultam o comércio eletrônico.

A vantagem de uma Intranet é o uso da interface gráfica pelo usuário, o que facilita o acesso às aplicações. Outra facilidade de uma Intranet é o fato de que o usuário pode utilizar o mesmo *browser* tanto para a Internet quando para a Intranet, com isto SOUZA (1999) afirma que não é necessário o investimento no desenvolvimento de aplicativos ou compra de pacotes de *groupware* de alto custo.

Para se implantar uma Intranet faz-se necessário que os sistemas operacionais de rede utilizados na empresa sejam compatíveis com aplicações da Intranet. SOUZA (1999) afirma que é necessário contemplar interfaces *sockets, gateways, APIs, drivers ou plug-ins* que são responsáveis pela tradução dos protocolos da Intranet (TCP/IP) e o protocolo mais utilizados nas redes como o IPX. Os sistemas operacionais mais conhecidos para a área são os: *Intranetware* e o *Windows*.

As *driver´s* APIs (*Aplication Program Interface*) ou *sockets*, são as interfaces entre os *browsers* e os aplicativos. Com o uso de um *browser* e de uma linguagem de programação tipo *Java*, SOAUZA (1999) afirma as empresas podem com um baixo custo, fazer a disponibilização de suas aplicações de banco de dados, planilhas, textos e outras, numa Intranet.

2. Intranets x Correio Eletrônico

As Intranets são consideradas entre outras coisas como um meio para colaboração entre os setores de uma empresa através do compartilhamento de informações. De forma que de acordo com BENETT (1997) as Intranets utilizam os correios eletrônicos como base para seu estabelecimento. Indo assim contra a filosofia dos *groupware* que vem para substituir o correio eletrônico.

O protocolo SMTP definido pela Internet é incorporado a tecnologia das *Webs*. Sendo assim a maioria dos navegadores da Web possuem a capacidade de enviar correspondência eletrônica de forma direta, sem a necessidade da utilização de um

programa específico para esta finalidade, trazendo assim uma enorme economia de tempo.BENETT (1997) afirma que isto "apresenta outras vantagens, como a eliminação da necessidade de instalar um programa específico de correio eletrônico em todos os computadores."

As Intranets oferecem além dos recursos de correio eletrônico através do navegador Web, a possibilidade também de acessar correios eletrônicos em outros *sites* Webs. Com isto BENETT (1997) chega a conclusão da constituição assim da base de uma categoria inteira de aplicativos bastante úteis, denominada automação do fluxo de trabalho.

3. As Intranets e o Groupware

BENETT (1997) diz que "o objetivo do *groupware* é "permitir que as pessoas trabalhem em conjunto através de comunicação, colaboração e coordenação", segundo um informe oficial da *Lotus Development Corporation* sobre o assunto."

As Intranets e os *groupwares* dependem da infra-estrutura de envio/recebimento de mensagens de correio eletrônico para que possam permitir a comunicação do tipo *store-and-forward*. Dedicam-se assim somente ao processamento de formulários e a fóruns de debate específicos.

Porém as Intranets e os g*roupwares* divergem em aspectos importantes:

- Enquanto os *groupwares* enfatizam o trabalho em equipe as Webs consideram os usuários isolados como seu público-alvo.

- Os *groupwares* utilizam o modelo "*push*" de distribuição de informações a partir de um repositório central, e as *Intranets* utilizam o modelo "*pull*" de

distribuição de informações, onde apenas os usuários interessados em uma informação vão a busca dela e a exibem.

BENETT (1997) afirma que "o *Lotus Notes*, um produto de *groupware*, é merecidamente famoso por sua capacidade interna de "duplicação", que permite que os usuários sincronizem os banco de dados. A obtenção do mesmo efeito através de Webs exige programação personalizada."

Os produtos desenvolvidos para os *groupwares*, tipo o *Lotus Notes* ou o *Novell Groupwise*, baseiam-se em componentes patenteados de banco de dados e de envio/recebimento de mensagens. Enquanto isto as *Webs* possuem sue produtos baseados em tecnologias de domínio público como o SMTP e o HTTP.

O *groupware* leva certa vantagem ao que se refere a segurança da rede e sua administração de dados distribuídos. Contudo para BENETT (1997) as *Webs* representam um menos custo, maior flexibilidade de uso e padrões abertos, comandando assim o interesse de grandes fabricantes de *software* garantindo então um rápido crescimento e desenvolvimento.

4. Gerenciamento de Documentos em uma Intranet

O grande acúmulo de papéis, registros, anotações, catálogos, protótipos desenhados em guardanapos durante o almoço, ou seja, de documentos, seu gerenciamento tornou-se uma tarefa desanimadora da era da informação.

Para BENETT (1997), "o gerenciamento de documentos tem estas quatro dimensões básicas":

- **Pesquisa/Recuperação –** capacidade de localizar o que você está procurando;

- **Segurança –** controlar o acesso a documentos para leitura/gravação;

- **Controle de versões –** acompanhar as alterações e os originais;

- **Arquivamento –** tornar dados históricos disponíveis.

Enquanto os sistemas de gerenciamento de documentos desempenham todas as funções descritas acima, as Intranets desempenham somente a função de pesquisa/recuperação. De forma que se uma empresa não necessita de um gerenciamento automatizado dos documentos, a opção mais simples é uma *Intranet*. Mas conforme BENETT (1997) caso todas as quatro funções mencionadas anteriormente sejam estratégicas na empresa, a opção é igualmente simples, basta adquiri ou desenvolver um sistema de gerenciamento de documentos.

BENETT (1997) afirma que: "no entanto, na grande área de interseção entre esses dois extremos, é ainda mais difícil tomar a decisão correta. Felizmente, as tecnologias são complementares, e os sistemas híbridos podem oferecer mais que a combinação delas".

5. O Funcionamento de uma Web Interna

5.1 TCP/IP: Uma Base de Rede de Baixo Custo

Comparando as Intranets e a Internet verifica-se que as maiores diferenças entre elas não estão relacionadas com a tecnologia, mais sim ao escopo, à mídia e às metas

que são aplicadas a esta tecnologia. Pois conforme BENETT (1997) disse, “a base da Internet e das Intranets é a família TCP/IP de protocolos de rede”.

5.1.1 TCP/IP e o IETF

O TCP/IP é uma pilha de protocolo não patenteada, de forma que nenhuma empresa ou outra instituição controla os padrões que compõem esta pilha. Porém de acordo com BENETT (1997) existe um grupo de pessoas anônimas que trabalham a fim de contribuir para evolução ta tecnologia e para o desenvolvimento da tecnologia da Internet, desenvolvem, documentam e discutem novos padrões de protocolo. É assim que a IETF (*Internet Engineering Task Force*) se define na RFC-1718.

Por ser um protocolo sem custo nenhum de licenciamento o TCP/IP pode ser utilizado por qualquer pessoa para desenvolver softwares de rede e comercializá-los cobrando apenas o custo da mão-de-obra. Sendo isto o que mais tem acontecido na Internet, e hoje em dia mais na WWW e nas Intranets. Já que empresas, estudantes, pesquisadores e aficionados vem de acordo com BENETT (1997) vem desenvolvendo softwares para a Internet durante décadas. O que mais surpreende é uma grande parte destes softwares se comparados com os vendidos comercialmente são tidos como superiores ou equivalentes.

Como o TCP/IP traz muitas vantagens custos para a tecnológica da Internet, torna então todos *sites* da Internet laboratórios para aplicativos TCP/IP, contribuindo assim para a rápida evolução e para a qualidade da tecnologia.

5.2 Endereçamento de Todos os Computadores

O endereçamento em uma intranet ocorre em dois níveis.

- Nível da rede: todo dispositivo tem um endereço IP.

- Nível do aplicativo: por localização de recursos, onde se costuma trabalhar, estando relacionada às convenções de atribuição de nomes.

Estes dois níveis de endereçamento são utilizados pois nem sempre a pessoa que esta trabalhando em uma rede sabe o endereço IP da máquina, somente o nome do recurso. Então este usuário ao digitar este nome em um formato reconhecido pelo computador, este utilizará um servidor de nomes (DNS) para fazer a localização deste endereço. Esta natureza de duas camadas de endereçamento para BENETT (1997) resulta em dois requisitos básicos de uma intranet:

- Atribuição de endereços IP a dispositivos de rede

- Estabelecimento de um serviço de atribuição de nomes.

Para se fazer uma atribuição de endereços IPs em uma rede utiliza-se uma das três maneiras a seguir:

- "Solicitar ao *InterNIC* um número (ou um bloco de números) exclusivo registrado para a sua empresa." (BENETT, 1997)

- "Atribuir a cada dispositivo um número não-repetido sem recorrer ao *InterNIC*." (ibidem)

- "Começa com uma faixa de endereços alocados por um dos dois métodos anteriores, mas adia a atribuição real de endereços a dispositivos até que uma solicitação seja feita. Quando isso ocorre, um servidor especial concede automaticamente um endereço IP temporário ao dispositivo que fez a solicitação. Isso é feito através do BOOTP ou do DHCP (*Domain Host Configuration Protocol*), que são extensões do TCP/IP projetadas

> especialmente para essa finalidade. Quando o dispositivo se desconecta da rede, seu endereço IP retorna ao pool e pode então ser atribuído a outro dispositivo.” (ibidem)

A distribuição de endereços através do endereçamento dinâmico, ou também chamado de atribuição instantânea, pode simplificar a inclusão de usuários na rede, já que não exige uma configuração de endereços em seu computador. Contudo este tipo de endereçamento segundo BENETT (1997) possui a desvantagem que “consiste na complexidade adicional no lado do servidor: deve ser mantido um processo especial para atribuir endereços durante o *login*.”

Com a utilização de recursos que possuem um nome e um endereço IP é necessário criar um catálogo de endereços, para tal existem duas maneiras conhecidas:

- DNS (*Domain Name System*), é usada para a Internet global e empresas maiores. O DNS está descrito na RFC 1123, seção 6.1, intitulada “*Domain Name Translation*”.

- Consiste em manter um arquivo central, normalmente denominado HOSTS, que mapeia nomes de host em endereços IP.

6. HTTP: Cliente/Servidor para o Restante do Pessoal

De acordo com BENETT (1997) “os termos cliente e servidor não se associam a um computador específico, nem permanecem o tempo todo associados a ele. Qualquer PC pode ser um cliente em determinadas situações e um servidor em outras, ou ambos ao mesmo tempo em relação a diferentes usuários.”

De forma que Cliente pode ser considerado um processo de computador que solicita serviços dos recursos de rede. Enquanto isto um Servidor é um processo de computador que presta serviços a solicitantes autorizados. Devido a isto então para BENETT (1997) o termo cliente/servidor refere-se sim a uma arquitetura computacional e não a uma tecnologia. Já que os aplicativos do tipo cliente/servidor podem ser implementados com a utilização de praticamente qualquer protocolo de rede, em qualquer sistema operacional e usando qualquer tipo de computador.

Com seu baixo custo o TCP/IP é tido como uma boa base para aplicativos cliente/servidor. Dando origem ao novo serviço do TCP/IP, o HTTP. Este novo serviço é uma ampliação da pilha do protocolo TCP/IP. De forma que aos computadores que oferecem suporte ao HTTP é dada a denominação de Servidores Web.

Estes servidores Web comandam a comunicação HTTP em uma rede. Oferecendo também um local natural para o armazenamento de páginas Web. Enquanto em alguns dos servidores Web incorporam ferramentas destinadas à organização e atualização do conteúdo, agregando assim valor às especificações do HTTP.

Os autores da W3 *Project* definiram o HTTP:

> *"HTTP é um protocolo no nível do aplicativo com a eficiência e a velocidade necessárias a sistemas de informação de hipermídia distribuídos e destinados à colaboração entre grupos de trabalho. Uma das características do HTTP é a definição e a negociação da representação de dados, que permitem a construção de sistemas independente dos dados que estão sendo transferidos."*

O HTTP então se trata de um protocolo padrão para comunicação que não necessita conhecer antecipadamente o tipo de conteúdo que transportará. Portanto não é

necessário também que o HTTP conheça o hardware ou o sistema operacional em que é utilizado. Se a plataforma oferecer suporte ao TCP/IP e à multitarefa, o HTTP pode ser utilizado nela.

7. Motivos para se ter uma Intranet

Ao se instalar uma Intranet deve-se levar em conta que ela é uma tecnologia que vem a ajudar aos funcionários e alavancar os negócios da empresa, e não ao contrário.

Para SOUZA (1999) os funcionários dentro de uma empresa poderão:

- Compartilhar e criar arquivos de uso diário.
- Ter acesso a informações e políticas da empresa.
- Efetuar comunicações e treinamentos via Intranet.
- Eliminar papéis que passam a circular eletronicamente pela rede.
- Compartilhar documentos e informações para a tomada de decisões.
- Ter uma interface única para acesso as aplicações na empresa.

Ao se elaborar um projeto para a implantação de uma Intranet é necessário de acordo com SOUZA (1999) verificar alguns quesitos:

- Projeto com cronograma, alocação de tarefas e orçamentos.

- Piloto e testes antes da instalação.

- Elaborar documentação de todos os processos a serem colocados na Intranet.

- Dar treinamento aos usuários.

- Montar equipe de suporte.

- Efetuar divulgação dentro da empresa, tendo obrigatoriamente o comprometimento e a ajuda da direção da empresa.

Após a elaboração deste projeto, deve-s e antes de partir para a implantação fazer uma avaliação de qual será o benefício que está intranet trará, ou seja, de acordo com SOUZA (1999) qual será o "*pay-back*", quais processos irão ser automatizados e agilizados, o que vai ser publicado nela e qual a economia de papel e processos resultantes.

Em uma Intranet para BENETT (1999) "as aplicações básicas iniciais, a serem implementadas numa Intranet, podem ser":

- Correio eletrônico.

- Consulta a manuais e documentos internos.

- Lista de ramais telefônicos.

- Boletins informativos e circulares.

- Avisos e normas como ISO-9000.

- Tabela de preços.

- Publicações (a Intranet e basicamente publicação).

- Formulários eletrônicos.

- Outros.

Com o objetivo básico de redução de custos a Intranet vem para economizar tempo e dar maior produtividade ao fluxo de trabalho, de forma que permita uma melhor tomada de decisões e melhor habilidade na resposta aos clientes. As empresas também poderão colocar documentações técnicas e informações sobre a manutenção de produtos para acesso via Internet, economizando assim custos.

Existem diferentes modelos de Intranet:

- Modelo multicamada: combina servidores públicos e internos, permitindo a comunicação entre os empregados da empresa e seus clientes.

- Modelo interno: formado de servidores de informação internos para acessos dos empregados a informações tecnológicas e treinamento. Esse modelo permite a eliminação de papel na empresa.

A implantação de uma intranet é tida como uma grande avanço para uma empresa, só que está ao implantar uma intranet deverá considerar também a implantação de um sistema de segurança "*firewall*" para isolar o trafego externo da Internet em relação a rede interna, evitando assim a entrada de intrusos, com o uso de senhas e programas de segurança. Para SOUZA (1999) "esses sistemas de segurança filtram a informação que trafega na rede, evitando a entrada de intrusos não autorizados".

BENETT (1999) afirma que "muitas empresas obtiveram economias de dezenas de milhões de dólares anuais com a implementação de Intranets, pela substituição de papeis, impressão gráfica e do transporte de documentos e manuais por meios eletrônicos da Intranet."

CAPÍTULO IV – SEGURANÇA NA INTERNET

1. Introdução

Hoje em dia com o avanço crescente da Internet e o fácil acesso a ela, torna-se cada vez mais necessário pensar-se em meios de manter as informações sigilosas seguras da melhor maneira possível, pois existem muitos criminosos de informática (normalmente garotos adolescentes) a solta pela Internet.

No início quando os invasores atacavam uma empresa e eram pegos, recebiam clemência dos tribunais através da alegação que eram jovens na tenra idade e não sabiam o que estavam fazendo, e utilizavam o argumento de que o material acabou sendo devolvido para a vítima. Contudo esta maneira de pensar nos dias de hoje mudou muito, pois a pessoa que é acusada de invadir um sistema e informações, não consegue se livrar mais com a alegação de que as informações foram devolvidas, pois ao contrário dos que roubam fisicamente as informações e necessitam de fotocopiadoras para fazerem as cópias e estas são facilmente identificáveis, no roubo digital a cópia dos arquivos pode ser feita inúmeras vezes e colocadas em locais diferentes ou enviadas via rede para outra pessoa, que fica difícil de saber se ao estar sendo devolvidas as informações, não exista nenhuma cópia desta em outro lugar. Devido a isto HAYDEN (1999) afirma que os arquivos digitais roubados são uma fonte de problemas, pois uma vez retirados, ninguém pode ter certeza se foram totalmente recuperados.

Desta forma serão expostas as maiores ameaças, e formas de ataques a uma rede ligada a Internet.

2. Ameaças

Com as crescentes conexões de redes a Internet existem inúmeras ameaças conhecidas a elas. Por tanto quando uma empresa resolve conectar-se a Internet deve-se proteger contra elas. Estas ameaças podem ser:

1. Ameaça de Repudiação: este tipo de ameaça ocorre quando um participante de uma transação que ocorre *online* pode vir a negar que a transação tenha realmente acontecido;

2. Ameaça à Transmissão de Dados: Este tipo de ameaça ocorre quando alguém intercepta a comunicação com a rede da empresa e consegue violar a confidencialidade e a integridade das informações;

3. Ameaças à Rede Corporativa: Ocorre quando a disponibilização dos serviços de Internet abri furos na segurança da rede, permitindo com que intrusos acessem outros componentes da rede interna.

4. Ameaças à Disponibilidade de Serviços: Ocorre quando é interrompida a disponibilidade de alguns serviços da rede, ou até mesmo da rede inteira, deixando seus legítimos usuários sem seus serviços;

5. Ameaças aos Servidores da Internet: Este tipo de ameaça ocorre quando um intruso penetra em um servidor de Internet e modifica as páginas e comandos que fazem com que este servidor funcione corretamente.

Com a utilização da Internet BERNSTEIN (1997) mostra através da Tabela a 2 os tipos de ameaças que atacam os aspectos vulneráveis da rede de computadores de uma

empresa e transmissões, quando as informações são trocadas entre a rede interna e a Internet.

Ameaças	Exemplo
Espionagem: a identidade de um (ou mais) dos usuários envolvidos em algum tipo de comunicação é observada para ser mal utilizada posteriormente. Informações confidenciais são observadas durante sua transmissão através da rede.	Farejadores de rede podem roubar IDs de usuários e senhas não-criptografadas enviadas durante sua transmissão em texto simples. Farejadores mais avançados podem roubar mensagens de correio eletrônico, transações da Web ou *downloads* de arquivos.
Disfarce: Um usuário finge ser outro. Se o usuário A assumir a identidade do usuário B, o usuário A será autorizado a utilizar os privilégios e direitos de acesso do usuário B.	Em um ataque de *spoofing* ao IP(Internet Protocol), os intrusos criam pacotes de dados com endereços de origem falsificados. Esse ataque explora aplicações que utilizam a autenticação baseada em endereços e permite o uso não-autorizado ao sistema destino e o acesso privilegiado a ele.
***Replay*:** Uma seqüência de eventos ou comandos é observada e reproduzida posteriormente para que possa efetivar alguma ação não-autorizada.	Falhas em esquemas de autenticação são exploradas juntamente com a falsificação de servidores de autenticação para subvertê-las.
Manipulação de Dados: A integridade dos dados é danificada durante o armazenamento ou durante a transmissão sem que isso seja detectado.	Devido a controles de acesso inadequados, os dados são modificados enquanto estão em um sistema. Da mesma forma, juntamente com as ameaças de disfarce e *replay*, as mensagens são interceptadas, modificadas e enviadas ao destinatário sem serem detectadas.
Roteamento Incorreto: Uma comunicação para o usuário A é roteada para o usuário B, o que pode levar uma interceptação de mensagem. Os roteamentos incorretos podem ser usados juntamente com disfarces, manipulações e *replays*.	Redes, linhas de comunicação e dispositivos desprotegidos ou inadequadamente configurados são suscetíveis a instruções de controle de roteamento não-autorizada, como o comprometimento de um provedor de serviços de internet.
Armadilha/Cavalo de Tróia: Um processo não-autorizado pode executar um programa como se fosse um processo	Procedimentos de gerenciamento de alteração inadequados nos quais programas de arquivos transferidos da Internet não

Ameaças	Exemplo
autorizado; um programa aplicativo ou de sistema é substituído por outro que contém uma seção adicional alterada, permitindo algum tipo de atividade mal-intencionada não-detectada.	têm seu código-fonte verificado
Vírus: Os vírus de computadores são códigos de programa que se auto-reproduzem. Eles se associam a um componente de um arquivo executável ou a um programa aplicativo de um sistema e posteriormente o modificam. Os vírus podem alterar ou eliminar diversos arquivos de sistema, alterar dados ou negar disponibilidade.	O uso ineficiente de programas de verificação de para: - unidades de disquetes (setor de inicialização e arquivos de dados) - arquivos de servidor (setor de inicialização e arquivos de dados) - arquivos de BBs e grupos USENET - mensagens ativas, como as que podem ser enviadas a partir de um sistema de correio eletrônico ou da Web
Repúdio: Um ou mais usuários negam ter participado de uma comunicação, uma ameaça critica para transações financeiras eletrônicas e acordos contratuais eletrônicos.	O comércio eletrônico, no qual as transações não incluem controles para: => origem => destino => tempo de entrega => prova de entrega
Negação de Serviço: O acesso a um sistema/aplicação é interrompido ou impedido, o sistema ou aplicação deixa de estar disponível, ou uma aplicação cujo tempo de execução é critico é atrasada ou abortada.	Uma “inundação de pacotes” pode esgotar a capacidade de uma rede ou sistema, tornado-o(a) não-disponível.

Tabela 2 - Classes de Ameaças (BERNSTEIN,1997 p. 29-30)

3. Tipos de Ataques

O protocolo utilizado na Internet é o TCP/IP para a transmissão de dados. Este protocolo foi projetado para possuir uma conectividade razoável, contudo sua segurança foi deixada de lado. Devido a isto as pessoas mal intencionadas da Internet descobriram inúmeras maneiras técnicas de driblar a segurança e causar panes nos equipamentos.

Existem segundo HAYDEN (1999) os ataques técnicos e os não técnicos, aonde os ataques técnicos se dividem em dois grupos TCP/IP, sendo eles:

=> Ataque de Negação de Serviço: estes tipos de ataques têm por objetivo desativar completamente os serviços do computador. Os mais conhecidos são: *SYN Flood*, *Ping* da morte, *Spoofing* ou falsificação de e-mail.

=> Ataque Furtivo: estes tipos de ataque têm como objetivo acessar um sistema de computador, que de outra maneira o usuário não teria acesso. Os mais conhecidos são: *Spoofing* de IP, Roubo de Senha através de Força Bruta e Seqüestro de Sessão.

Enquanto isto os ataques não técnicos mais conhecidos são:

- Engenharia social;
- Usuário enrolado ou papel colado no fundo do Teclado;
- Computador Desprotegido;
- Mergulho no lixo ou vale a pena picotar.

3.1 Ataques técnicos

Este tipo de ataque ocorre quando é necessário o conhecimento técnico na área de informática para conseguir chegar ao objetivo final. São os ataques mais utilizados e de maior produtividade para o invasor, pois não existe a necessidade de sua presença física no local do ataque.

3.1.1 Ataques de Negação de Serviço

SYN *Flood*: Para se estabelecer uma conexão TCP/IP faz-se necessário que ela se inicie com uma solicitação do sistema cliente para o sistema servidor, caso esta solicitação seja válida o servidor irá completar a conexão. Desta forma para HAYDEN (1999) cada conexão deverá ser reconhecida para que o ataque seja diagnosticado.

Como para responder as solicitações de conexão existe a necessidade de ocupar alguns recursos do servidor (um pouco de memória e uma pequena parte do tempo do processador) os intrusos utilizam-se disto para derrubar o servidor.

Este ataque ocorre da seguinte forma: é enviada uma enorme quantidade de solicitação de conexão para o servidor, em geral sem um número de IP de retorno, ficando assim difícil de identificar o computador que está enviando o ataque. Possui como resultado a negação de serviços, já que o servidor está tão ocupado respondendo a solicitações de conexão que não consegue fazer mais nada, ficando assim parcialmente ou totalmente sem condições de utilização. Este tipo de ataque é combatido na maioria dos sistemas operacionais através de *pacth* de correção.

***Ping* da morte:** Este tipo de ataque ocorre quando um usuário mal intencionado envia uma mensagem *ping* e faz modificações no tamanho do pacote que possui como valor máximo o de 65.536 *bytes*. Este pacote ao ser recebido pelo servidor derruba-o, o

sistema pode congelar e precisar ser reiniciado ou pode haver uma pane total no servidor. É tido como um ataque infantil e incômodo.

Os sistemas operacionais possuem correções para os serviços de ICMP dos *softwares* de protocolo TCP/IP dos servidores. Segundo HAYDEN (1999) *ping* é o nome do aplicativo que utiliza o *Internet Control Message Protocol (ICMP)* , e funcionado como um sonar que envia um pacote e aguarda a resposta, caso não haja resposta significa que o computador está indisponível.

***Spoofing* ou Falsificação de E-mail:** este tipo de ataque é tido como muito infantil. Ele ocorre quando um usuário inscreve o endereço de outro em inúmeras listas de *newsgroup* da USENET, e quando o servidor de e-mail da pessoa começa a receber a grande quantidade de e-mails direcionados ao usuário ele se sobrecarrega e entra em pane.

O *Spoofing* também pode ser utilizado como um ataque furtivo, quando um intruso modifica o cabeçalho de uma mensagem de e-mail como se o chefe de uma pessoa estivesse solicitando uma senha para trabalhar num sistema, quando esta estiver fora do local de serviço.(HAYDEN, 1999).

3.1.2 Ataques Furtivos

Spoofing de IP: este tipo de ataque ocorre quando um intruso simula possuir um IP confiável para o servidor.

Ocorre da seguinte maneira: temos o cliente A, o servidor B e o Invasor X. Aonde o cliente A possui um endereço IP confiável para o Servidor B. O ataque inicia-se com o Invasor X simulando possuir o endereço IP do cliente A, solicitando uma conexão com o Servidor B, de forma que ao receber a solicitação B reconhece o solicitação e estabelece números de seqüência.

Após isto o servidor B mandará uma resposta ao cliente A para reconhecimento dos números de seqüência. Nisto entra o intruso X que tentará adivinhar o número de seqüência enquanto envia mensagens para A, pois este não poderá receber a mensagem de B e responder negando a solicitação de conexão.

Este tipo de ataque para BERNSTEIN (1997) é tido como uma estratégia desajeitada e entediante, contudo uma análise recente revelou que umas ferramentas existentes podem executar um ataque de *Spoofing* de IP em menos de 20 segundos. É um ataque perigoso, e ocorre cada vez mais.

Roubo de Senha através da Força Bruta: é o tipo de ataque mais comum que existe, mais lento e exige muito trabalho e inúmeras vezes tornam-se improdutivo. Para que ele ocorra é necessário um servidor que não desconecta após várias tentativas de acesso malsucedidas. Porém mesmo que o servidor faça a desconexão existem maneiras de se automatizar o processo.

Este tipo de ataque ocorre quando se possui um *login* conhecido e um dicionário eletrônico para tentar diversas senhas diferentes para este *login*. Segundo HAYDEN (1999) isto é um processo entediante e caso esteja sendo feito uma auditoria na rede ele é facilmente detectado e cancelado, de tal forma que torna o roubo de senha bem difícil.

Seqüestro de Sessão: parecido com o *Spoofing* de IP este ataque ocorre quando um intruso consegue monitorar uma sessão existente entre o cliente A e o servidor B, tomando conta da identidade de A, derrubando-a e assumindo suas funções na sessão com B, com os mesmos privilégios de A. segundo HAYDEN(1999) este tipo de ataque é de difícil proteção.

3.2 Ataques não Técnicos

Estes tipos de ataques ocorrem quando o intruso não necessita de conhecimentos na área de Informática, em geral é necessária a presença física do invasor no local que será feito a invasão por meio tecnológico mais tarde.

Os ataques são:

Engenharia Social: ocorre quando os invasores trabalham com a natureza humana, tornando-se um ataque bastante traiçoeiro. Em geral utiliza-se a hierarquia de comando para que possa receber uma senha, pois um funcionário acaba passando a senha a invasor quando este finge ser um superior na hierarquia de comando da empresa. Este tipo de ataque segundo HAYDEN (1999) ocorreu muito durante as décadas de 70 e 80, pois as pessoas ainda não estavam acostumadas com a informática, hoje em dia torna-se mais difícil a utilização deste tipo de ataque.

Usuário enrolado, ou papel colado no fundo do teclado: este tipo de ataque ocorre mesmo que o sistema de segurança das informações de uma empresa seja o mais seguro possível, mas se o usuário não sabe como proceder com sua senha da melhor maneira possível acaba deixando-a anotada em um papel colado embaixo do teclado, ou até mesmo escrita em bilhetinho na sua estação de trabalho, então um invasor que consiga um emprego nesta empresa, encontra esta senha e dependendo do nível de acesso que ela disponibiliza, o estrago está feito.

Computadores Desprotegidos: é de conhecimento que uma rede para ser segura necessita de *firewalls*, *proxys* e outras ferramentas de segurança, contudo caso os servidores não possuam uma segurança física, estejam longe do alcance de pessoas que possam estar trabalhando na empresa só para conseguir acesso aos dados, ou seja em vez de estarem em salas abertas ou em armários de fácil acesso, deverão ser colocadas em salas fechadas com acesso restrito e com senha de proteção de tela.

Mergulho no lixo, ou vale a pena picotar: este tipo de ataque ocorre quando o invasor revolve o lixo da empresa a procura de *login* de acesso e de senhas. Hoje em dia é pouco utilizado, pois a maioria das empresas procura picotar seus documentos antes de joga-los ao lixo.

4. Políticas de Segurança

Uma empresa para ter segurança em seus sistemas deverá em primeiro lugar criar políticas de segurança, que segundo BERNSTEIN (1997), "são diretivas de gerenciamento que estabelecem as metas comerciais da organização, fornecem uma estrutura de responsabilidades e domínios aos processos".

Na elaboração das políticas de segurança deve-se levar em consideração os seguintes princípios, de acordo com SOARES (1995):

- **Autenticação:** este princípio rege os termos e forma de autenticação de um usuário para ter acesso a uma rede. Com a autenticação o sistema possui a garantia de que quem está tentando o acesso é uma pessoa autorizada.

- **Controle de acesso:** através do controle de acesso o sistema irá permitir ao usuário conectar e acessar os dados e as partes do sistema que lhe são permitidas e autorizadas.

- **Confidencialidade:** a confidencialidade é a garantia de que a comunicação entre o usuário e o sistema é de maneira tal que os outros usuários não consigam ter acesso aos dados trocados entre o usuário e o sistema

- **Integridade:** a integridade garante que os dados acessados pelo usuário não se modifiquem enquanto estão sendo transportados pela rede.

- **Não repúdio:** este serviço serve para garantir que as solicitações do usuário ao sistema sejam respondidas positivamente se este tiver autorização para executa-las.

5. Segurança do Correio Eletrônico

Os serviços de correio eletrônicos existentes hoje na Internet baseiam-se no protocolo SMTP conforme a norma da RCF 822 da Internet. Este serviço não foi definido com sistemas de segurança. Desta forma para BERNSTEIN (1997) este serviço pode sofrer inúmeras ameaças, podendo ser divididas em dois grupos: as ameaças a mensagens em trânsito e as ameaças aos agentes de entrega de mensagens em sistemas finais.

5.1 Ameaças a Mensagens em Trânsito

As ameaças a Mensagens em trânsito ocorrem quando uma pessoa forja um e-mail solicitando algo para outra como se fosse o chefe desta, esta pessoa acaba obedecendo a ordem e envia dados.

Este problema ocorre, pois o SMTP reflete muito dos problemas de segurança da Internet. Para BERNSTEIN (1997) estes problemas são:

- **Falta de Confiabilidade:** A falta de confiabilidade não é uma preocupação para as informações públicas, mas torna-se inaceitável para a comunicação comercial confidencial;

- **Falta de autenticidade:** Em uma mensagem de correio eletrônico não existe a possibilidade de saber se a pessoa está utilizando e informando seus dados corretamente, desta forma não se pode identificar com quem se está conversando;

- **Falta de Integridade:** Não existe a possibilidade de garantir que uma mensagem que foi enviada estará correta ao ser recebida;

- **Falta de não-repudiação:** Com os sistemas de correio eletrônicos existentes os usuários não podem negar que enviaram uma mensagem, contudo podem negar o conteúdo desta mensagem.

5.2 Ameaças aos agentes de entrega de mensagens em sistemas finais

Estes tipos de ameaça dividem-se em dois subtipos, sendo eles conforme BERNSTEIN (1997):

- **Inicialização Automática de Aplicações através do MIME:** este tipo de ameaça ocorre quando um interpretador gráfico do MIME é configurado para abrir/executar programas fora dele de acordo com as mensagens recebidas. Estas mensagens poderão conter vírus ou comandos que possam abrir as portas de um computador para os invasores.

- **Ataques em *Hosts* através de Agentes de Correio Eletrônico:** Este tipo de ameaça ocorre com o *Sendmail*, que é o sistema de e-mail mais utilizado nas plataformas UNIX. Ele possui mais ou menos dez mil linhas de códigos e uma infinidade de *bugs* e *back doors* que deixam os servidores vulneráveis aos ataques dos invasores, de forma que pode deixar o servidor todo aberto para quem conseguir e quiser faze o que bem entender.

6. Segurança dos Servidores de *News*

As empresas que utilizam os servidores de *News* na sua grande maioria de acordo com BERNSTEIN (1997) não dão muita importância para a segurança dos servidores

pois acham que o *News* é um serviço que não apresenta ameaça a segurança por ser um conjunto de BBSs pelos quais os funcionários podem trocar mensagens.

Contudo o *News* é baseado no protocolo NNTP (*Network News Transfer Protocol*), que é semelhante ao SMTP e possui comandos para enviar mensagens entre servidores de *news*, e também entre os servidores e os leitores finais.

Desta forma as ameaças aos servidores podem ser dividas da seguinte forma:

- **Interrupção do *News*:** este tipo de ameaça ocorre quando uma pessoa mal intencionada envia artigos fajutos para publicação no lugar de artigos verdadeiros,, ou através de comandos impossibilita que outros publiquem seus artigos no servidor.

- **Violações de Políticas:** Este tipo de ameaça ocorre quando um funcionário pode publicar em um *news* amplamente lido informações confidenciais da empresa, ou também o *news* receber informações agressivas e publicá-las para todos os grupos.

- **Ameaças à Empresa:** os serviços de *News* se não forme bem configurados podem abrir brechas na seguram da empresa e deixar seus sistemas expostos a quem quiser fazer algo de ruim.

7. Segurança dos Servidores de Terminal

Os servidores de terminal utilizam o protocolo *telnet* para fornecer serviços de *login* remoto a outro *host*, para este *login* são utilizados e controles de ID de usuário e uma senha padrão, conforme seria em um acesso local.

Enquanto isto existem também comandos de *shell* do tipo r-, *rlogin* e *rsh* que fornecem também recursos de *login* remoto a outras máquinas. BERNSTEIN (1997) disse que "... ao contrário do *telnet*, esses serviços não utilizam o mecanismo de autenticação utilizado pelo programa de *login* local..."

Os comandos do tipo r- fazem o uso de um mecanismo que irá simular um "acesso confiável", dando assim possibilidade de certos usuário terem acesso a rede sem necessidade de *login* e senha. Este acesso disponibiliza, segundo BERNSTEIN (1997) , a um grupo limitado de usuários que possuam seus nomes de conta, tanto no diretório local ou no diretório principal, acesso privilegiado a todo o sistema.

Desta forma o acesso a sistemas através do *telnet* ou *rlogin* dá acesso *shell* direto ao sistema, diferente do FTP e do Correio eletrônico.

8. Protocolos de Segurança

8.1 IPSEC (*IP Security*)

O IPSec (IP *Security*) é um conjunto de protocolos padrão com o intuito de garantir comunicações privadas seguras em redes IP. Ele garante confidencialidade, integridade e autenticidade nas comunicações de dados através de redes públicas IP.

O IPSec é utilizado para fornecer uma solução ponto-a-ponto em uma arquitetura de rede, pois sua implementação possui a encriptação do nível de rede e autenticação. Com a utilização do IPSec não a necessidade de que os sistemas fim e as aplicações precisem sofrer qualquer mudança para obter a vantagem de uma boa segurança, já que os pacotes encriptados enviados são vistos como pacotes IPs comuns, podendo ser facilmente passados através de qualquer rede IP, sem que seja feita a mudança de qualquer equipamento intermediário. Desta forma, somente os dispositivos do *host* final é que deverá entender a encriptação.

Seu funcionamento baseia-se em um novo conjunto de *headers* que serão adicionados ao datagrama IP. De acordo com JÄHN (2001) “estes novos *headers* são colocados após o *header* IP e antes do protocolo de nível 4 (Transporte), fornecendo informações para a segurança dos dados dos pacotes IP”. Estes *headers* são:

- *Header* de Autenticação (AH): ao ser adicionado a um datagrama IP, o *heard* de autenticação garante a integridade e a autenticidade dos dados, incluindo os campos invariáveis no *header* IP externo. Contudo não garante proteção da confidencialidade. De forma que o AH utiliza preferencialmente uma função "*keyed-hash*",pelo motivo da tecnologia de assinatura digital ser lenta e reduzir assim o desempenho da rede..

- Dados de Segurança Encapsulados (ESP): o *header* de segurança quando adicionado a um datagrama IP, irá dar proteção a confidencialidade, integridade e autenticidade dos dados. Caso o ESP seja utilizado para validar a integridade dos dados, ele não inclui os campos invariáveis no *header* IP.

Para JÄHN (2001), “o AH e o ESP podem ser usados independentemente ou juntos, apesar de que para a maioria das aplicações apenas um deles é suficiente.” O IPsec não possui uma definição de algoritmo especifico para ambos os protocolos, porém oferece uma estrutura aberta para a implementação de algoritmos padronizados.

As implementações do IPSec em sua grande maioria utilizam os modelos de criptografia MD5 da RSA *Data Security* ou o algoritmo *Secure Hash* (SHA).Para JÄHN (2001) “o DES é, atualmente, o algoritmo de encriptação mais comumente oferecido, contudo RFCs indicam o uso de muitos outros sistemas de encriptação, incluindo o IDEA, o *Blowfish* e o RC4.”

8.2 SSL (Secure Sockes Layer)

O SSL (*Secure Sockes Layer*) é uma solução que fornece serviços de segurança genéricos para os diversos protocolos TC/IP, uma vez que protege os protocolos das camadas inferiores.

Com o fornecimento de uma estrutura de segurança aonde os protocolos das aplicações podem ser executados, o SSL tenta dar proteção a toda pilha TCP/IP.

O SSL, segundo BERNSTEIN (1997), é composto de dois protocolos:

- Protocolo de Registro: responsável por transmitir os dados reais;

- Protocolo de *Handshake*: responsável por negociação das técnicas a serem utilizadas no fornecimento de serviços de segurança, que inclui confidencialidade e autenticidade

8.3 PGP (Pretty Good Privacy)

O PGP (*Pretty Good Privacy*) foi criado no final dos anos da década de 1980 por Phil Zimmermann que garantia a segurança de sistemas de correio eletrônico. No início foi distribuído livremente entre seus conhecidos, e a partir de 1991 passou a ser distribuído livremente pela internet.

Este programa foi rapidamente adotado por várias pessoas, passando a frente do PEM, pois era independente da plataforma do sistema operacional. Por ser independente dos agentes de correio eletrônico sua imigração para várias plataformas torna-se mais fácil.

O PGP utiliza um único conjunto de algoritmos responsáveis por garantir a confidencialidade, integridade e autenticidade. De acordo com BERNSTEIN (1997), "o PGP também permite a compactação de mensagens externas por meio do utilitário Zip".

O funcionamento do PGP é através de um método bem menos formal para o gerenciamento de chaves e de acesso confiável do que o utilizado pelo PEM. Ele utiliza dois "chaveiros"; onde um é utilizado pelo usuário para armazenar seu próprio par de chaves, e o outro chaveiro irá armazenar as chaves públicas de que tem conhecimento.

Para BERNSTEIN (1997) "o primeiro chaveiro é armazenado criptografado com uma "frase de acesso" conhecida apenas pelo usuário". Enquanto isto "o segundo chaveiro contém certificados PGP, compostos apenas por uma chave pública e um nome associado". Desta forma no PGP não existe o conceito de CAs, mas sim a confiança de um usuário no outro e a possível confiança do primeiro usuário nos que são confiados pelo outro. Podendo assim o usuário ter o discernimento de confiar ou não nas outras pessoas.

8.4 PEM (Privacy Enhanced Mail)

O protocolo PEM (*Privacy Enhanced Mail*) surgiu no ano de 1990 quando o *Privacy and Security Research Group* da IETF (*Internet Engineering Task Force*) começou o desenvolvimento de um padrão de segurança para ser utilizado nos correios eletrônicos. Este protocolo é definido segundo BERNSTEIN(1997) de acordo com a forma que os "...agentes de criptografia de chave pública, gerenciamento de certificados e correio eletrônico devem se integrar para formar um sistema de segurança de correio eletrônico."

Os certificados utilizados pelo PEM são baseados no X.509, que acabaram se tornando um padrão para certificados de chave pública. Estes certificados são dispostos de uma forma hierárquica restrita, aonde as CAs (*Certification Authorities*) garantem as

identidades de pessoas e seus certificados, enquanto isto os certificados das CAs são emitidos pelas PCAs(*Policy Certification Authorities*) e os certificados das PCAs são assinados por um único certificado-raíz pertencente a IPRA (*Internet Policy Registration Authority*). Estes certificados segundo BERNSTEIN(1997) possuem o tempo de validade de acordo com o especificado pelas Cas.

BERNSTEIN (19997) afirma que "através do padrão PEM, uma única mensagem pode ser enviada a vários destinatários através do uso de uma única chave de sessão, para criptografar dados, e da inclusão de varas cópias dessa chave". Uma mensagem com cabeçalho PEM só poderá ser aberta por quem souber a chave para descriptografa-la.

8.5 SSH (Secure Shell)

O SSH (*Secure Shell*) é um programa que foi desenvolvido para ser utilizado no acesso a computadores remotos. Possui como maior diferença para o *Telnet* o trabalho com senhas criptografadas, possuindo assim uma conexão segura, já que no *telnet* a senha não é criptografada e circula pela rede da maneira que é digitada.

Este programa possui como maiores características:

- Todas as conexões são criptografadas de forma transparente e automática;

- Protege o DISPLAY das sessões (conexões X11);

- Pode criptografar outros serviços, por exemplo, ftp, tftp, etc.

- Protege as conexões contra cavalos de tróia, DNS *spoofing*, *routing spoofing*, IP spoiofing.

O SSH foi desenvolvido com o propósito de substituir o *rlogin*, *rsh*, *rcp* e as maiorias das funções existentes no *Telnet*, já que prove uma comunicação mais segura entre duas máquinas.

8.6 HTTP Seguro

Em junho de 1994 a *CommerceNet Consortiun* cria um padrão chamado de *Secure* HTTP (S-HTTP), funcionando como uma extensão do HTTP. Este padrão fornece bastante flexibilidade ao aceitar algoritmos, gerenciamento de chaves, certificados e normas de segurança, para BERNSTEIN (1997) então o S-HTTP oferece compatibilidade com vários sistemas.

No S-http as mensagens possuem estruturas semelhantes as do PEM. Estes formatos das mensagens podem ser utilizados para a distribuição de certificados, sendo desta forma uma alternativa para as pessoas recuperarem certificados através de outros mecanismos.

Os S-http possui como maior diferença as normas que os clientes e os servidores utilizam para se conectar, de forma que pode exigir ou não que um determinado serviço de segurança seja utilizado. BERNSTEIN (1997) diz que “essa flexibilidade torna-se extremamente benéfica ao montar a estrutura para que o uso do S-HTTP seja difundido”.

9. Criptografia

A partir da necessidade de se enviar informações sigilosas em meios de comunicações não confiáveis, foi que surgiu a criptografia.

As criptografias são métodos utilizados para modificar o texto original da mensagem que deve ser transmitida. Os textos são criptografados na origem e depois enviados.

Quando o texto criptografado chega ao destino, ele é decriptado e então lido. Contudo desta maneira se o intruso descobrir o método utilizado ele quebrará o texto codificado e terá acesso as informações.

Com esta falha surgiram os métodos que utilizam chaves de codificação para criptografar o texto. Sendo eles: criptografia com chave pública e criptografia com chave secreta.

9.1 Criptografia com Chave Secreta

Este tipo de criptografia utiliza uma chave secreta que deverá ser de conhecimento tanto do emissor quanto do receptor.

Os métodos que utilizam a mesma chave secreta para criptografar ou decriptar um texto são denominados de simétricos ou de baseados em chave secreta.

Este tipo de criptografia possui como seu algoritmo mais conhecido o DES (*Data Encryption Standard*).

9.1.1 DES (Data Encryption Standard)

Este método foi desenvolvido pela IBM e depois de adotado pelo governo do EUA como padrão.

SOARES (1995) e TANENBAUM (1997) afirmam que o DES codifica blocos de 64 bits de um texto normal gerando então 64 bits de texto criptografado.

Funcionamento de um algoritmo de codificação DES segundo SOARES (1995):

- Parametrizado por uma chave K de 56 *bits*, possui 19 estágios diferentes (Figura 1a)

- 1º Estágio: transposição dos bits do texto independente da chave;

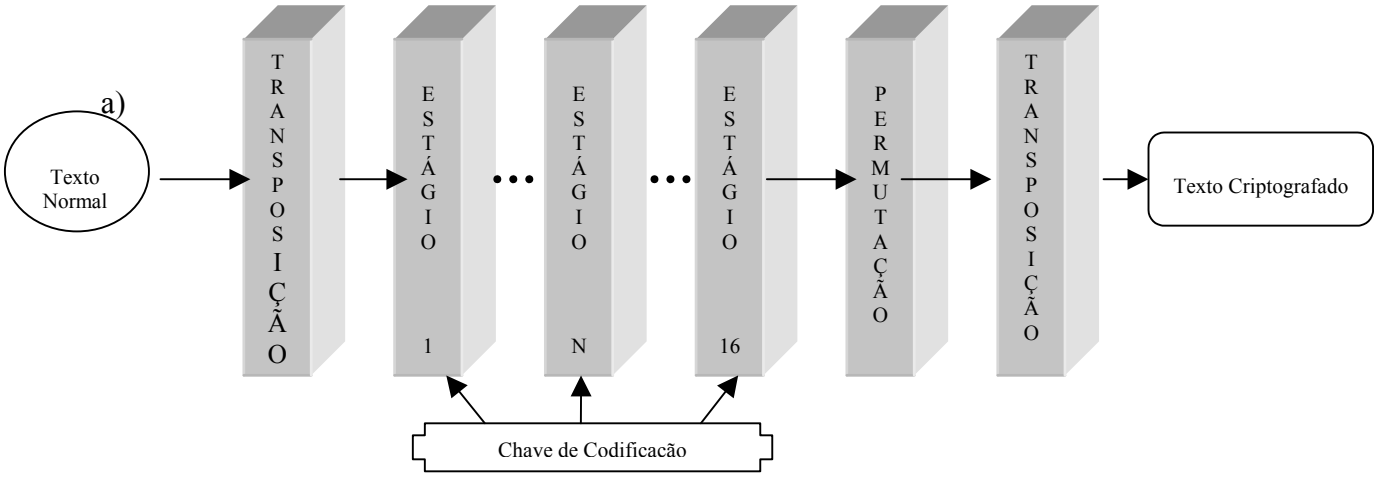
- 2º ao 17º Estágio: são praticamente identificados (transposições e substituições), possuindo como parametrização as chaves Ki, obtidas pela aplicação de funções i para outro, nos bits da chave K original (Figura1b);

- 18º Estágio: realiza a permutação dos 32 bits mais significativos com os 32 bits menos significativos do bloco de dados;

- 19º Estágio: realiza uma transposição inversa a do primeiro estágio.

Para a decodificação do texto é necessário somente executar os estágios de trás para frente.

a)



b)

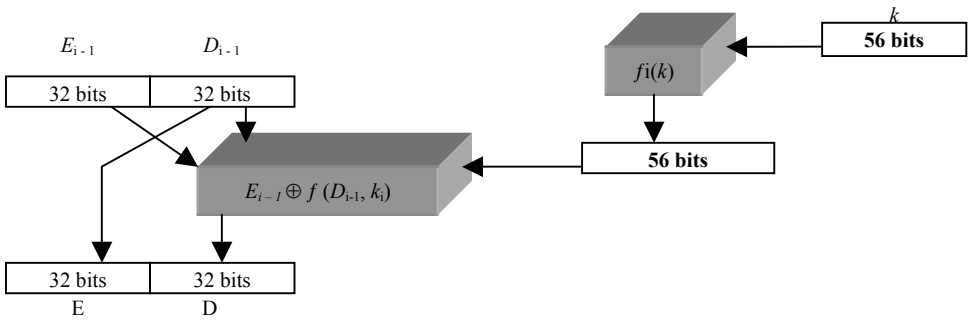


Figura 2 Método de Criptografia DES (SOARES, 1995)

Este método possui como principal problema à necessidade que os envolvidos saibam o valor da chave a ser utilizada na encriptação e decriptação do texto, de forma que SOARES (1995) exemplifica dizendo que em uma empresa aonde existam *n* funcionários e eles se comunique m utilizando chaves em pares é necessário que um funcionário conheça n² números de chaves, tornando-se assim inviável.

Descrição de outros Algoritmos Simétricos:

Algoritmos	Descrição
Triple DES	O 3DES é uma simples variação do DES, utilizando-o em três ciframentos suscessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	O *International Data Encryption Algorithm* foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM *Systec*. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.
Blowfish	Algoritmo desenvolvido por Bruce Schneier, que oferece a escolhe entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou-o no Twofish, concorrente ao AES.
RC2	Projetado por Ron Rivest (o R da empresa RSA *Data Security Inc*.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail

	utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor do RC4, RC5 e RC6, este último concorrente ao AES.

Tabela 3 - Algoritmos de Criptografia Simétricos (MAIA,2001)

9.2 Criptografia com Chave Pública

No ano de 1976 foi proposto um novo método que revolucionava os sistemas de criptografia. Este método proposto por DIFFIE e HELLMAN era baseado na utilização de chaves distintas, nas quais uma era para codificação (E) e a outra para decodificação (D), de forma que a derivação de D a partir de E fosse impossível ou muito difícil de ser realizada de maneira prática.

Quando for respeitada está condição poderá ser tornada pública a chave E. desta forma os métodos que possuem esta característica são denominados de assimétricos, ou baseado em chave pública.

Desta maneira SOARES (1995) afirma que "a diferença entre os métodos de criptografia simétricos e assimétricos, é que, nos primeiros, a chave K usada no procedimento de codificação é igual a chave K' usado no procedimento de decodificação, isto é, K=K', e nos assimétricos K≠K' ".

O método assimétrico utilizado é o RSA (*Rivest, Shamir e Adleman*)

9.2.1 RSA (Rivest, Shamir e Adleman)

Este método de criptografia é tido como o mais importante na criptografia assimétrica. é baseado na dificuldade de fatoração de números muito grandes.

De acordo com SOARES (1995) para que possa ser usado o RSA, é necessário tomar dois números primos *p* e *q*, após obter um número *d*, tal que *d* e *(p-1)*(q-1)* sejam

primos entre si, ou seja, que o número *d* satisfaça a equação máximo divisor comum *[d,(p-1)*(q-1)]=1*.

Em seguida é necessário obter um número *e* tal que *e*d=1 (mod[(p-1)*(q-1)])*, de forma que a divisão de *e*d* por *(p-1)*(q-1)* seja igual a *1*.

Após as equações anteriores estarem satisfeitas, poderá se utilizar um par (*e,n*) para chave pública e um par (*d,n*) para chave privada. Com as chaves é feita a codificação e decodificação.

$C \leftarrow P^e \pmod n$

$P \leftarrow C^d \pmod n$

Com este tipo de criptografia o usuário só precisa guardar a chave pública do outro para enviar uma mensagem criptografada. E esta só poderá ser aberta com a chave privada.

A seguir na tabela 4 visualizamos outros Algoritmos de Criptografia Assimétrica:

ElGamal	O *ElGamal* é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento

	nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie e Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie - Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Tabela 4 - Algoritmos de Criptografia Assimétrica (MAIA,2001)

10. Firewalls

No início a internet era pequena e não havia a necessidade de se preocupar com a segurança. Contudo com o elevado crescimento da internet tornou-se necessário a criação de bloqueadores de acesso entre uma rede e outra. Assim sendo surgiram os *Firewalls* (portas contra fogos).

Os *firewalls* são então utilizados para proteger as redes antes que invasores possam fazer estragos na rede coorporativa. Tornou-se assim uma ferramenta estratégica para a implantação de uma política de segurança em uma rede.

Estes tipos de serviços oferecem geralmente proteção contra ataques a protocolos ou a aplicações individuais, protegendo também contra ataques de *spoofing*, são também de fácil configuração, oferecendo relativa flexibilidade para que as

configurações ofereçam restrições para diferentes tipos de tráfegos, ou seja, um *firewall* recebe um pacote verifica o que fazer com ele, se deixa entrar ou não na rede.

Os *firewalls* podem ser utilizados para esconder umas máquinas das outras e regular o tráfego que entra e sai das máquinas.

O *firewall* é um único ponto de entrada de uma rede, contudo caso ele seja invadido, torna-se assim um único ponto de falha na segurança, pois dá acesso a toda a rede.

Para SOARES (1995) os *firewalls* possuem algumas limitações:

- os *firewalls* não garantem a integridade dos dados;
- os *firewalls* não garantem a autenticidade da origem dos dados;
- a maioria dos *firewalls* não garante o sigilo dos dados.
- os *firewalls* não garantem proteção contra ameaças internas;
- um *firewall* é apenas um ponto de entrada para uma rede.

10.1 Técnicas de *Firewall*

Existem três tipos de *firewalls* que podem ser utilizados: filtros de pacotes baseados no roteador e no *host*, filtro "inteligentes" baseados no *host* e *gateways* de aplicações baseadas no *host*.

Para que a segurança seja mais forte é feita uma combinação destas técnicas de *firewalls*.

10.1.1 Filtros de Pacotes

Tipo como a maneira mais fácil de se implantar um software é feita em um roteador que conecta a rede interna a internet ele utiliza o conceito de filtragem de pacotes para fazer o controle do tipo de tráfego que poderá passar pelo roteador.

No início eles eram utilizados para fazer o controle da largura de banda que as conexões poderiam utilizar. Estes tipos de filtros são implantados na maioria das vezes sem que o usuário final tenha conhecimento da existência deles.

A técnica de filtragem de pacotes é simples, e baseia-se na tecnologia "*Store-and-forward*" (armazenamento e encaminhamento) dos roteadores, ou seja, quando um host ou roteador receber um pacote em uma interface, ele terá suas informações de cabeçalho comparados com um conjunto de filtros, para que então, seja decidido se o pacote pode passar, se o pacote será abandonado inteiramente ou, se será "rejeitado" (neste caso será enviada uma mensagem ICMP de volta ao ponto de origem).

Para SOARES (1995) a maioria dos filtros de pacotes levam em consideração os seguintes critérios:

- A direção do tráfego (da interface para a rede interna ou da rede interna para a interface);

- A interface na qual o tráfego foi recebido ou para o qual se destina;

- O tipo de protocolo;

- Os endereços IP de origem e de destino;

- A informação sobre o “estado” do TCP.

Os fornecedores de roteadores na sua grande maioria já incorporam os filtros de pacotes no software de seus roteadores.

Um filtro de pacote possui com sua sintaxe:

Lista	Ação	Prot.	Origem	Destino
Access-List1	Deny	TCP	All	Inside por 23

A onde:

- Lista: lista de acesso

- Ação: *permit* ou *deny*

- Prot.: protocolo a ser utilizado

- Origem: local da solicitação

- Destino: destino da solicitação.

Contudo os filtros de pacotes possuem limitações com o controle dos pacotes, pois um *firewall* não poderá ficar verificando minuciosamente o conteúdo de um pacote, pois irá trazer uma que da no desempenho da rede.

10.1.2 Filtros "Inteligentes"

De acordo com SOARES(1995) os filtros inteligentes são baseados em *hosts* e desempenham também as mesmas funções gerais dos filtros de pacotes padrão, por~em possuem maior funcionalidade e não apresentam parte dos problemas dos filtros de pacotes padrão.

A maioria dosa filtros inteligentes são dotados de uma interface GUI administrativa para facilitar na configuração dos filtros de pacotes. Esta interface deixa de lado a necessidade do conhecimento de uma linguagem misteriosa, para receber entradas em um formato legível e amigável, transformando então para uma linguagem de máquina.

A maioria dos filtros inteligentes segundo SOARES (1995) possuem heurísticas para verificação das regras, de maneira que uma não interfira na outra. Estes filtros também possuem vários níveis de *log*, que podem variar desde uma simples contagem dos pacotes a um mecanismo que aciona o administrador caso algum tipo de evento aconteça.

Os filtros inteligentes na sua maioria aceitam autenticação, por se basearem no *host*. Essas autenticações podem ser do tipo *telnet* e FTP.

11. PROXY

Os servidores *proxy* em contrapartida dos *firewalls* adotam a abordagem "*store-and-forward*" na qual encerram a conexão de chagada a partir da origem e iniciam uma nova conexão para o destino.

Para isto, os servidores em geral possuem várias interfaces de redes para comunicar-se com várias redes, funcionando quase como um *gateway* de base dupla, ou seja, é uma máquina que pertence a duas redes distintas e as máquinas existentes nesta rede não se conversam diretamente, somente passando pelo *Proxy*.

11.1 Servidor *Proxy* de Aplicação

O servidor *proxy* segundo SOARES (1995) facilita a vida do usuário, pois estabelece a segunda conexão com a máquina remota para o usuário, evitando assim a necessidade do usuário acessar o sistema operacional no *firewall*.

Os servidores *proxy* oferecem várias vantagem em relação aos *gateways* de base dupla, sendo eles:

- Não exige que o usuário tenha acesso ao sistema operacional;
- Não exige que o usuário faça várias conexões através de diferentes máquinas;
- Dão impressão de que a conexão é completamente transparente após esta ser estabelecida;
- "escondem" o *host* interno do servidor de destino, sendo considerada a maior vantagem.

Os servidores *proxy* em geral são de três tipos:

- servidores *proxy* de aplicação específica: este tipo de servidor é utilizado conforme o nome diz, para um tipo de aplicação específica. Apesar de parecer um pouco limitada, ela trás a possibilidade de decisões da aplicação específica;

- servidor *proxy* genérico: este tipo de *proxy* é tido como um *packet relay* que aceita as conexões recebidas. Ele consulta então alguns tipos de tabela de configuração para que venha a saber quais são as conexões permitidas, então assim sendo irá estabelecer a conexão com o seu verdadeiro destino;

- servidor *proxy* de circuito: este tipo de servidor permite que vários usuários se comuniquem com vários servidores, oferecendo assim uma transparência completa tanto para o usuário, quanto para o servidor, criando assim um circuito virtual fim a fim entre o cliente e o servidor.

Os servidores *proxy* possuem como limitações:

- falta de transparência;

- necessidade da criação de um servidor *proxy* específico para cada aplicação.

Desta forma os servidores *proxy* não são uma solução definitiva para a segurança, mas em combinação com os *firewalls* tornam-se de grande valia.

CAPÍTULO V – MODELO DE SEGURANÇA

1. Introdução

A partir dos estudos efetuados nos capítulos anteriores partiu-se para a elaboração do modelo para a implantação de segurança para uma Intranet. Para tal torna-se necessário uma classificação dos tipos de Intranet, níveis de segurança e serviços á serem protegidos, pois uma Intranet implantada sem dispositivos de segurança é um livro aberto para todos.

Os principais motivos para uma Intranet não ser considerada segura são:

- Funcionários que provém da população em geral, podendo ter pessoas má intencionadas;

- A população possui uma parcela significativa de harchers, vândalos e oportunistas;

- Contratação de profissionais autônomos que não possuam vinculo total com a empresa e acaba ocorrendo às vezes uma rotatividade muito grande;

- Nem todas as Intranet's são internas;

- A Internet pode ser usada como uma Wan para conexão entre filiais, expondo a rede da empresa a toda comunidade da Internet;

- Corre o risco de remoção ou substituição acidental dos dados.

Com isto deve-se então definir o que proteger e como proteger.

2. Serviços a Disponibilizar

Com estudo feitos através de visitas a empresas para ter o conhecimento do que esta se utilizando nas Intranets, defini-se a seguir os serviços a serem disponibilizados na Intranet.

2.1 Serviço de Autenticação

O primeiro serviço a ser disponibilizado em uma Intranet é a autenticação. Este serviço é responsável pelo controle de quem pode utilizar a rede. Ele é baseado em um login e uma senha, que deve ser mantida pelo usuário em segredo, não deixando que outros descubram.

Devido a isto, a senha merece algumas considerações especiais para a sua escolha.

2.1.1 A Escolha de uma Senha

Para que uma senha seja considerada boa, ela deve ter no mínimo 8 caracteres entre letras, números e símbolos, ser facilmente decorada e de difícil digitação. Os sistemas em geral diferenciam letras maiúsculas de minúsculas.

Deve-se evitar a utilização de sobrenome, número de documentos, placas de carros, números de telefones e datas relacionadas com o dono da senha, já que são informações de fácil obtenção, dando assim melhor liberdade para os criminosos.

Outra regra para a criação de senhas é não utilizar palavras conhecidas de dicionários de qualquer língua, pois os criminosos em geral utilizam programas para quebra de senha que pesquisam em dicionários palavras conhecidas.

2.1.2 Mudança de Senha

A mudança de senha deve ser feita periodicamente para garantir uma melhor segurança e nunca deve ser feita por algum funcionário responsável pelo serviço, mas sim pelo próprio dono da senha.

2.2 Serviço Web

O segundo serviço a ser disponibilizado em uma Intranet é o serviço Web disponibilizado pelo servidor de Intranet. Este serviço é utilizado para elaboração dos sistemas a serem rodados na empresa.

Pode ser considerado o alvo principal dos ataques em uma empresa, pois sem o serviço de Web a empresa pode parar seus serviços. Existem muitos tipos de ataques à este tipo de serviço, sendo os mais conhecidos:

- *Syn flood* : Quando ocorre uma grande quantidade de pedidos de conexão sem um endereço IP para retorno da resposta da solicitação (HAYDEN, 1999).

- *Ping* da Morte: Ocorre quando é feito o envio de mensagens *ping* com pacotes maiores do que o valor máximo de 65.536 bytes. Quando este pacote é recebido pelo servidor, derruba-o(HAYDEN,1999).

- *Backdoors*: os sistemas operacionais na sua grande maioria possuem *backdoors*, que são falhas na programação que deixam abertas fendas nos servidores para a invasão de *harckers*.

Como se vê, os ataques a serviços de Web baseiam-se quase sempre em defeitos de fabricação dos softwares. Então, para que se proceda uma melhor segurança para este serviço é necessário ficar alerta para atualizações e *patches* de correção lançados pelos fabricantes de software.

Outra maneira de se proteger o sistema é a utilização de um *firewall* que filtre os tipos de pacotes que podem chegar ao servidor. Também se deve manter um programa antivírus no servidor.

2.3 Serviço de DNS

O serviço de DNS torna-se necessário para a Intranet, pois é através dele que se tem o endereço de cada computador interno e como localizar os computadores externos quando a Intranet é conectada a Internet.

Este tipo de serviço ao ser atacado e colocado fora do ar deixa os equipamentos sem achar o servidor e os sistemas param de funcionar.

Para escapar deste tipo de problema o servidor de DNS deverá estar abaixo de um servidor principal, geralmente o provedor de acesso. Também é necessário instalar um *firewall* para bloquear o acesso não autorizado.

2.4 Serviço de FTP

Este serviço, se não for bem configurado, pode ser crítico para a segurança da Intranet.

Um ponto importante na disponibilização do serviço de FTP é a utilização ou não do FTP anônimo, já que com este tipo de FTP qualquer usuário poderá ter acesso SHELL ao sistema. A maioria das empresas descarta a utilização do FTP anônimo, já que existem muitos erros nos servidores de FTP que abrem brechas no sistema.

Contudo, outras empresas passam a utilizar programas de FTP criptografados, a partir do qual torna-se mais difícil o acesso ao sistema. Existem também empresas que utilizam o FTP via HTTP no servidor.

2.5 Serviço de Telnet

O serviço de telnet oferecido nas empresas é utilizado para acesso remoto ao servidor, sendo que o principal usuário é o administrador da rede. São poucos os usuários que se utilizam do Telnet, de forma que pode ser considerado um serviço a menos para disponibilizar na rede.

2.6 Serviço de Correio Eletrônico

Este serviço é o mais utilizado pelas Intranet's, já que elimina o deslocamento do funcionário de um setor para o outro. Porém, é um dos serviços que mais traz problemas para a Intranet de uma empresa, pois é através dele que a maioria dos vírus, *back door* e *worms.*

2.6.1 Correio Eletrônico: O Alvo

A maior parte das empresas utilizam os correios eletrônicos para troca de informações entre seus empregados, dependendo do porte da empresa, também são utilizados para a troca de mensagens entre matriz e as filiais , e também com seus clientes e fornecedores. Em geral estas mensagens possuem um conteúdo sigiloso, tornando-as alvo dos *harcker's*.

A vulnerabilidade dos correios eletrônicos é evidenciada através duas ameaças conhecidas:

- Inicialização automática de aplicações através do MIME: ocorre quando um agente de correio eletrônico executa automaticamente uma mensagem que contenha vírus ou *backdoor*.

- Ataque em *hots* através de agentes de correio eletrônico: estes tipos de ataques ocorrem quando o sistema utilizado para correio eletrônico possui *bug's* e *backdoor's*, já que o sistema mais utilizado é o *sendmail* que possui vários problemas, este ataque é o mais comum.

Existe também uma nova forma de ataque aos servidores de correio eletrônico, conhecida como "SPAM". Este tipo de ataque ocorre quando uma pessoa recebe inúmeros *emails*, que em geral são propagandas, lotando sua caixa de entrada. Como geralmente o SPAM é enviado para diversos usuários do mesmo servidor em grande quantidade, não dando tempo para o servidor processar as informações, acabando assim por provocar seu travamento e sua queda, deixando o serviço fora do ar.

Outro grande problema dos correios eletrônicos é a utilização por funcionários de má índole, pois estes podem se aproveitar desta situação e enviar informações sigilosas da empresa para a concorrência.

2.7 Serviço de Banco de Dados

As empresas estão utilizando cada vez mais Banco de Dados para guardar informações necessárias para um bom andamento, e também sigilosas, tendo então que ser protegidas.

Os servidores de banco de dados possuem em geral autenticadores próprios, existido então um *login* específico para utilização do sistema, esta autenticação deve levar em conta também às recomendações das senhas de autenticação na rede, não sendo iguais.

Os principais ataques aos servidores é a tentativa de cópia de dados da empresa, derrubada do servidor, parando os sistemas, ou até mesmo apagar as informações armazenadas em seu interior, podendo trazer inúmeros problemas.

3. Tipos de Intranet

Para uma melhor dinamização do trabalho optou-se pela criação de perfis de Intranet's, tentando abranger todas as Intranet's existentes. A elaboração destes perfis levou em consideração os serviços disponibilizados e a conexão com a Internet.

Com isto chegou-se a três perfis de Intranet, sendo eles:

- Intranet Pura

- Intranet Intermediária

- Intranet E-Commerce

3.1 Intranet Pura

Este tipo de Intranet pode possuir desde somente o serviço de autenticação e web como todos os outros serviços. Foi denominada de Intranet Pura, pois não possui conexão com a Internet, existe somente na empresa, e é utilizada somente por seus funcionários. (Figura 3)

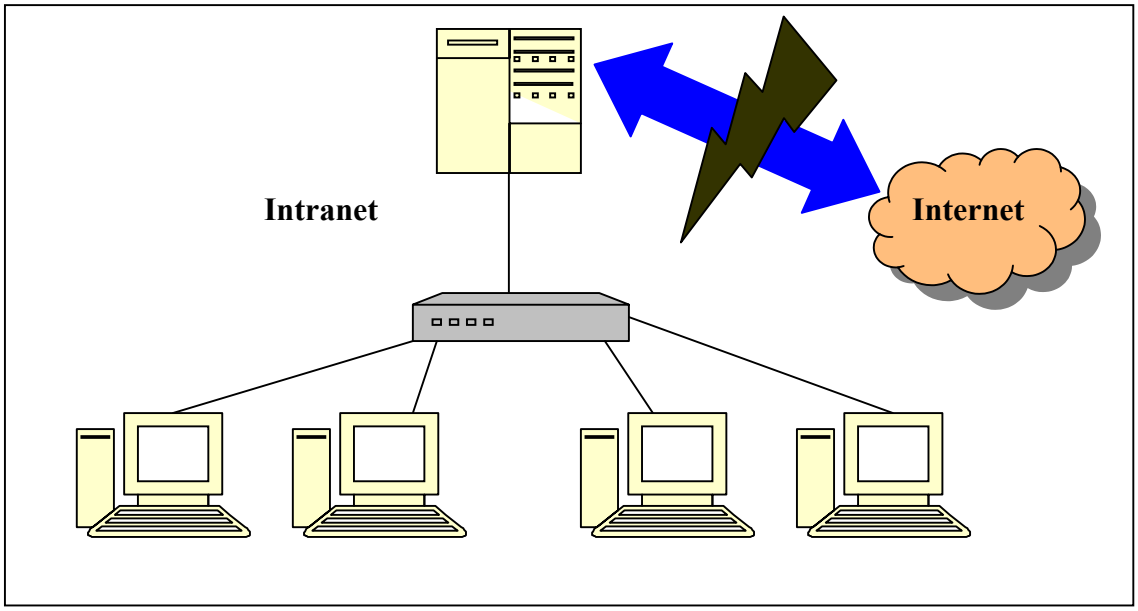


Figura 3 Intranet Pura

3.2 Intranet Intermediária

Este tipo de Intranet passa a utilizar os serviços da Internet para conexão entre a matriz e as filiais, tornando-se assim um alvo em potencial para ataques externos, de maneira que se aumenta a preocupação com o sistema de segurança. Podendo também possuir acesso de pessoas fora da empresa. (Figura 4)

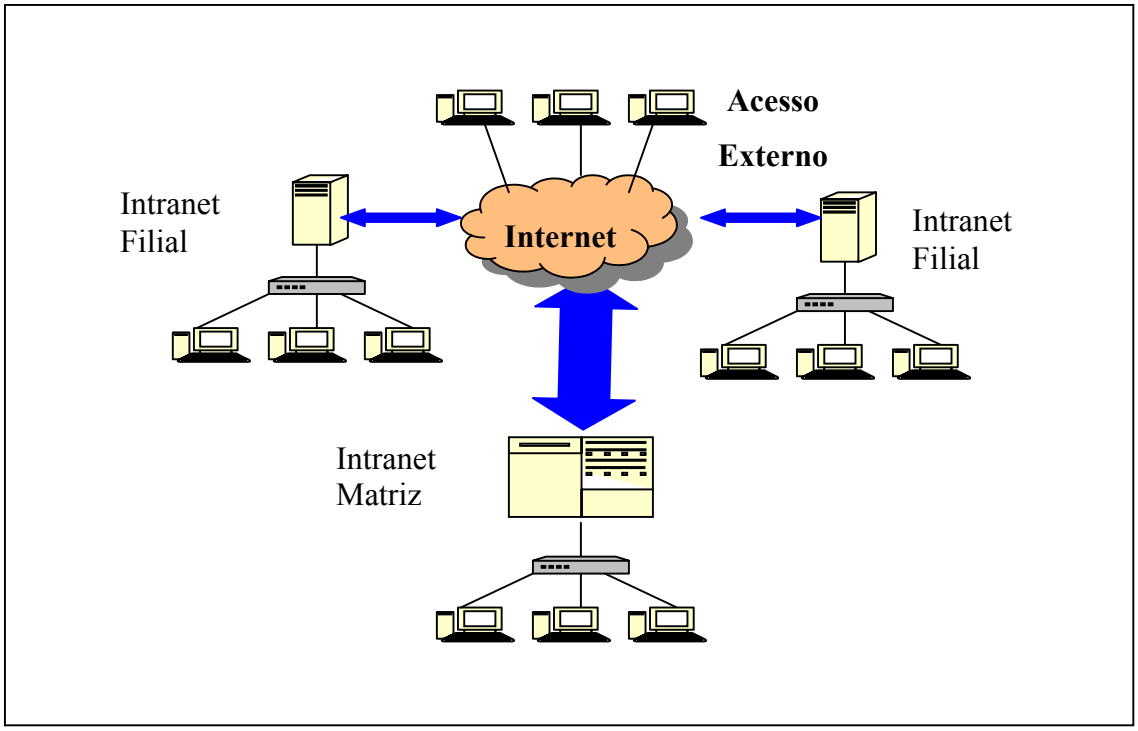


Figura 4 Internet Intermediária

3.3 Intranet E-Commerce

Este tipo de Intranet é o mais complexo de todos. Além de possuir os serviços disponibilizados pelos perfis anteriores de Intranet, ela disponibiliza o comércio eletrônico para seus clientes, de maneira que torna-se o tipo de Intranet que mais gera preocupação quanto a segurança. (Figura 5)

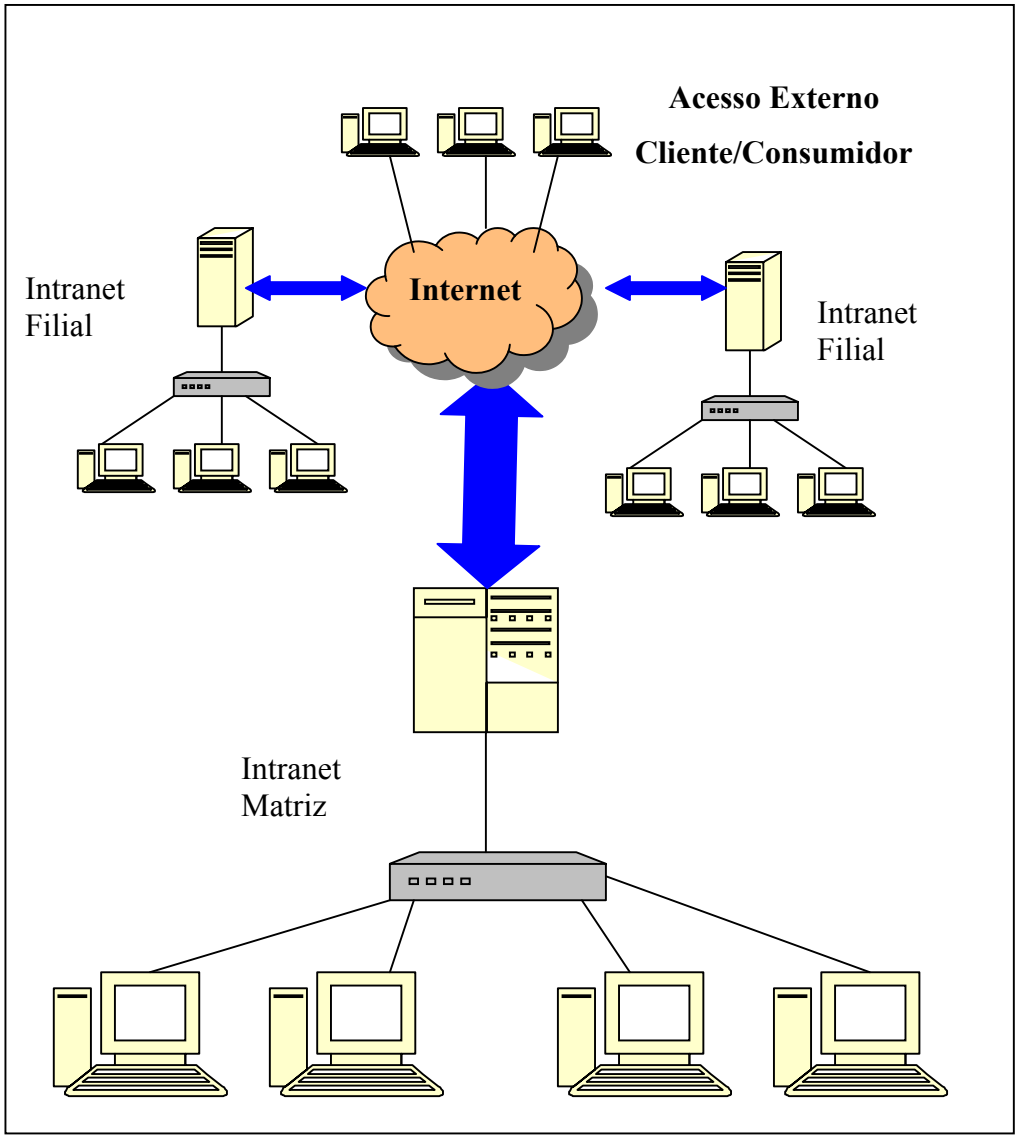


Figura 5 Intranet E-Commerce

4. Níveis de Segurança

Com a utilização da Intranet torna-se necessário a definição de níveis de segurança de acordo com o perfil de Intranet, sendo assim definiu-se os níveis de segurança para estudo como:

- Nível Básico

- Nível Intermediário

- Nível Avançado

Estes níveis se diferenciam de conforme o tipo de Intranet que ele protege, sendo que em ordem de proteção começa pela Intranet Pura, seguida pela Intermediária e por fim a E-Commerce.

5. Como Proteger os Serviços?

Após os estudos sobre os serviços a serem oferecidos pelos diferentes tipos de Intranet, torna-se necessário à definição de como proteger cada serviço.

5.1 Serviço de Autenticação e Web

Os ataques aos servidores de autenticação e Web partem da iniciativa da quebra de senhas utilizadas para acesso a estes. Estes ataques partem do conhecimento do *login* de um usuário válido, sendo necessário somente descobrir a senha deste usuário. A proteção deste tipo de serviço vária de acordo com, o tipo de Intranet. Para tal define-se os meios de proteção:

- Intranet Pura: neste tipo de intranet como não existe a conexão com a Internet é necessária somente à utilização de autenticadores que utilizem senhas criptografadas e também uma política de troca de senhas periodicamente.

- Intranet Intermediária: este tipo de Intranet por ser um pouco mais avançada, e ter acesso à Internet passa a ter a necessidade de utilizar além de um autenticador de senhas com criptografia, um *firewall*, podendo ser físico ou lógico, o qual deve ser configurado para permitir acesso as áreas restritas somente aos endereços IP's confiáveis.

- Intranet E-Commerce: este é o tipo mais avançado de Intranet, por se tratar de comércio via Internet, é necessário um avançado projeto de segurança. Este tipo necessita além do autenticador criptografado e o *firewall*, a utilização dos softwares de HTTP seguro, scripts de segurança, e um constante monitoramento da rede.

5.2 Serviço de DNS

O serviço de DNS somente é atacado quando for bem sucedido o ataque ao servidor Web e de Autenticação, pois este é mais um serviço disponibilizado no servidor Web, de maneira que a alteração ou derrubada do servidor de DNS é feita em um único ataque.

Este tipo de ocorrência é pouco comum em uma Intranet Pura, pois somente é utilizado dentro da empresa. A partir do instante que passa a ter conexão entre a Intranet e a Internet torna-se mais propenso os ataques a este serviço, já que quando fora do ar os equipamentos não se encontram.

Para solucionar este tipo de problema é necessário que existam dois possíveis servidores de DNS, sendo que um deve ser o servidor Web e o outro o servidor do provedor de acesso a Internet, desta maneira sempre terá um em funcionamento.

5.4 Serviço de Correio Eletrônico

Os serviços de correio eletrônico são um dos mais visados para ataques, existem várias maneiras de atacá-los, contudo está cada vez mais crescendo os estudos referentes a sua proteção. Os mais avançados são os que utilizam os conceitos de chave pública, porém de acordo com BERNSTEIN(1997) existem questões a serem levantadas:

- Gerenciamento de Certificados. Quase todas as aplicações de criptografia de chave pública produzidas em grande escala utilizam certificados para verificar assinaturas; porém, existem algumas diferenças na maneira em que esses certificados são gerenciados.

- Modelo de Acesso Confiável. Diversas aplicações, como o PEM, utilizam uma hierarquia de certificados. Outras como o PGP, preferem adotar um *bottom-up* e fazem com que pessoas assinem as chaves públicas.

- Compatibilidade com Outros Padrões. Devido à natureza instável do correio eletrônico, , fundamental que uma solução para a segurança de correio eletrônico seja compatível com especificações de multimídia, como o MIME.

- Recurso de Distribuição a vários Destinatários. Atualmente, o paradigma de correio eletrônico não pode ser considerado completo sem se levar em conta o grande número de listas de debates que permitem o envio por difusão de mensagens a vários usuários.

- Encaminhamento de mensagem. Se uma mensagem for enviada assinada e criptografada a um destinatário, essa pessoa poderá encaminhar a mensagem a outrem. Nesses casos normalmente é desejável conservar a assinatura na mensagem ao remover o envelope de criptografia.

Desta Forma alem de utilizar as tecnologias do PEM e do PGP, visto nos capítulos anteriores, existem também dois novos métodos de segurança, sendo eles:

-MOSS (MIME *Object Security Services*): criado pela IETF, é baseado quase que totalmente nas especificações do PEM, com algumas vantagens segundo BERNSTEIN(1997), sendo elas: não exige o uso de certificados para verificar chaves,

não exige que os usuários tenham nomes diferenciados e, não exige que as mensagens sejam assinadas antes de criptografadas.

- S/MIME: criado pela *RSA Data Security*, , uma tentativa de incluir segurança do padrão MIME através da definição de novos conte£dos MIME. De acordo com BERNSTEIN(1997) ele não está vinculado a uma hierarquia de certificação, e sim a uma tentativa de definir um padrão de criação de mensagem usando certificado X.509, deixando os detalhes de gerenciamento de certificados para os implementadores.

Após o levantamento destas discussões notou-se que é necessária a utilização da tecnologia de criptografia de chave publica para os três perfis de Intranet, os dispositivos de segurança que são diferenciados é em relação à utilização de um Antivírus e um bloqueador de SPAM nas Intranet's Intermediária e na Intranet E-Commerce, já que na Intranet Pura as mensagens trafegam somente dentro da empresa.

5.5 Serviço de FTP

A utilização do serviço de FTP na Intranet Pura é necessário para a colocação de documentos em um local de fácil acesso aos empregados, este tipo de serviço ao ser disponibilizado deve ser devidamente configurado de forma que os usuários tenham somente acesso aos documentos que lhes competem e não possam acessar locais.

No caso das Intranet's Intermediárias e E-Commerce, é necessário avaliar profundamente a necessidade da liberação do FTP Anônimo para os clientes, já que o acesso SHELL ao servidor abre inúmeras situações de risco, de forma que a melhor solução seria a utilização de um FTP com acesso restrito aos endereços IP's dos equipamentos internos. E para a disponibilização de arquivos para os clientes a utilização de um FTP via HTTP, que torna mais seguro.

5.6 Serviço de Banco de Dados

O serviço de Banco de Dados disponibilizado em uma Intranet Pura corre somente o risco de uma má utilização pelos usuários, ou ainda também a copia de informações pelos usuários em disquetes, *zip disk's*, cd's e entrega para pessoas externas a empresa.

A partir do momento que a Intranet passa a ter conexão com a Internet é que surgem as invasões aos bancos de dados, para tal torna-se necessário seguir uma política de segurança para o Servidor de Banco de dados. Esta política deverá levar em conta os seguintes itens:

- Servidor de Banco de Dados separado do Servidor Web e de Autenticação;

- *Log's* de auditoria em todas as transações;

- Políticas de Backup;

- Utilização de um firewall definindo quais os endereços IP's que podem ter acesso ao banco;

Com a utilização da Intranet E-Commerce é necessário deixar o acesso externo no servidor externo somente a partir de funções e scripts existentes no servidor Web, não dando acesso direto aos clientes.

6. Esquemas de Segurança

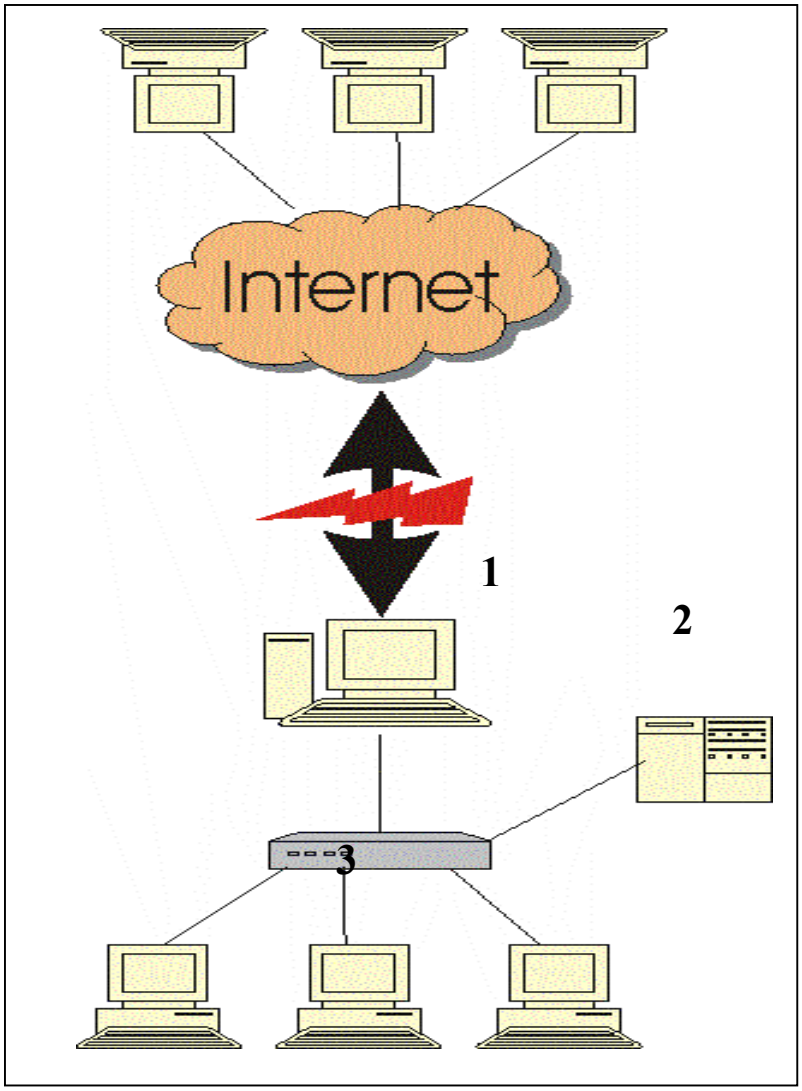


Figura 6 Esquema de Segurança de Intranet Pura

Este esquema de segurança, na figura 6, demonstra como ser feita a instalação de uma Intranet Pura, onde cada número denomina os seguintes equipamentos, e suas configurações:

1 – Servidor Principal: neste servidor serão disponibilizados os serviços da Intranet: Serviço de Autenticação, Web, DNS, Telnet, FTP e Correio Eletrônico, em sua

configuração deverão ser utilizados os critérios vistos nas seções anteriores, sendo eles: criptografia de chave publica, PGP ou PEM, criptografia na autenticação.

2 – Servidor de Banco de Dados: necessário a utilização de um servidor separado para uma melhor performance da rede.

3 – Estações de trabalho: Utilização de programas com autenticação criptográfica;

Após a visualização do Modelo de Segurança para Intranet Pura, veremos o modela a ser utilizado pela Intranet Intermediária, que está representado pela figura 7. Neste modelo passa a existir a conexão da Intranet com a Internet de modo que é necessária uma ampliação dos dispositivos de segurança, para tal ficou definido a seguinte estrutura:

1 – Servidor Principal: este servidor será igual ao da Intranet Pura, contudo para uma melhor proteção utilizará um *Firewall,* este *firewall* poderá ser tanto lógico quanto físico, dependendo das necessidades da empresa e das verbas a serem utilizadas, para tal recomenda-se fazer um estudo do tipo de *firewall.*

2 – As filiais da empresa também possuíram um servidor que fará a conexão entre suas estações e a matriz. Este equipamento também possuirá um firewall que impeça o acesso direto a sua rede.

Com o decorrer do crescimento se houver necessidade deve-se dividir os serviços disponibilizados para outros servidores, mas que todos estejam atrás do *firewall* do servidor principal.

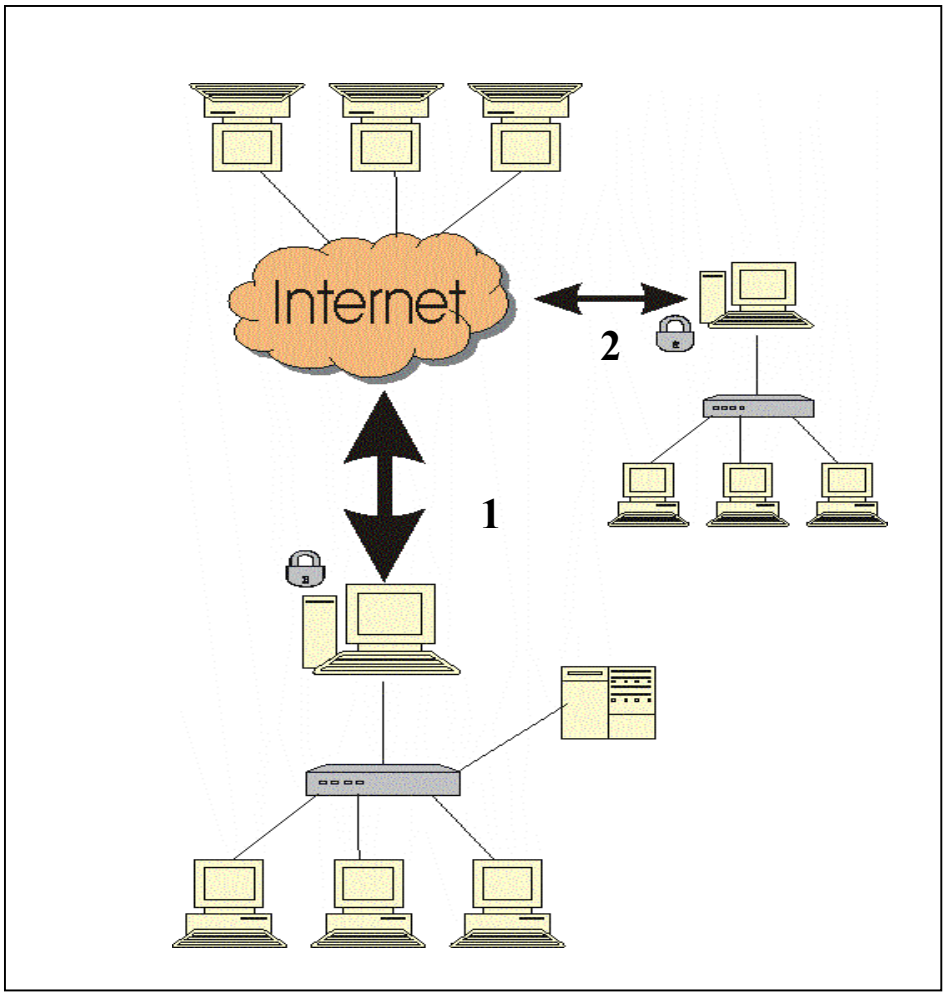


Figura 7 Esquema de Segurança Intranet Intermediária

A partir do momento que a empresa passa a disponibilizar o comércio eletrônico para seus clientes, passamos então a utilização da Intranet E-Commerce, este tipo de intranet é a existente principalmente em Bancos e Lojas de departamentos. Com este tipo de intranet é necessária a utilização do maior número de dispositivos de segurança. Com isto, além dos dispositivos utilizados nos modelos de Intranet Pura e Intermediária é necessária a utilização de protocolos seguros, por exemplo, HTTPS para que haja uma maior confiança dos clientes.

Os dados a serem transportado pela Internet deverão ser criptografados para que não haja o risco de serem interceptados e utilizados por criminosos. Estes dados ao serem armazenados no servidor de banco de dados deverão ser bem guardados para em caso de invasão não poderem cair nas mãos dos bandidos. (Figura 8)

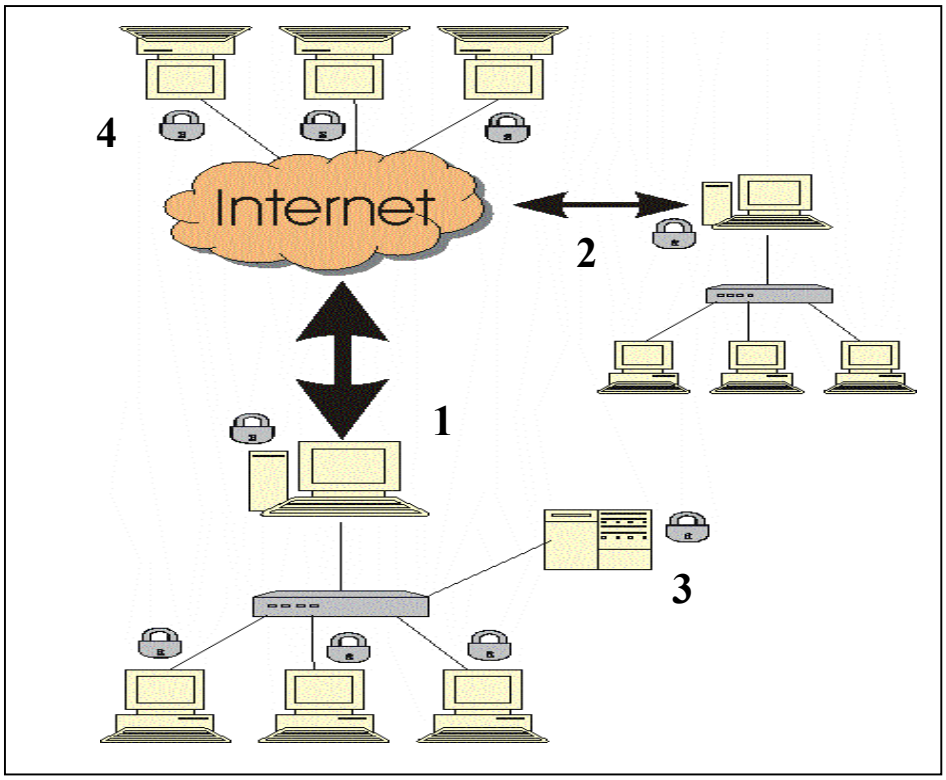


Figura 8 Esquema de Segurança Intranet E-Commerce

CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES

Neste trabalho foram propostos diversos esquemas de segurança voltados aos diferentes perfis de Intranets. Para a definição destes esquemas, levou-se em consideração, em primeiro plano, as diversas ameaças a um sistema de informações que podem surgir a partir do ambiente externo (por exemplo, a Internet) ou mesmo dentro da organização (como no caso de usuários desavisados ou mal intencionados).

Num outro nível de pesquisa, foram estudados os diversos serviços que podem ser disponibilizados no contexto de uma Intranet e a partir destes foram definidos os diferentes perfis que foram igualmente levados em conta para fins de definição dos esquemas de segurança.

Finalmente, foram levados em conta os mecanismos atuais que contemplam as diferentes formas de proteção possíveis em sistemas computacionais conectados em redes, particularmente aqueles vinculados a redes públicas como no caso da Internet.

Com os resultados publicados neste documento, espera-se ter trazido uma contribuição à área de projeto de desenvolvimento de Intranets, procurando oferecer uma guia que permita ajustar corretamente os mecanismos de proteção adequados a cada grupo de serviços que deverão ser disponibilizados no contexto de uma Intranet.

Apesar de existirem mecanismos diversos conhecidos incorporados a ferramentas e/ou equipamentos conhecidos no mundo, neste trabalho optou-se por não vincular nenhum esquema de proteção a alguma ferramenta conhecida. Preferiu-se deixar por conta do profissional envolvido no desenvolvimento da Intranet a escolha de que ferramenta adotar, até porque esta escolha depende também da plataforma utilizada para implantar os servidores diversos da Intranet.

No que diz respeito a sugestões para futuros trabalhos, propõe-se os seguintes tópicos:

- Investigar os diversos esquemas de segurança num ambiente de implantação, procurando gerar situações de ataque e verificar a eficiência dos mecanismos propostos;

- Analisar as ferramentas disponíveis no mercado do ponto de vista dos mecanismos propostos neste trabalho para estabelecer que ferramentas enquadrariam-se melhor aos diferentes esquemas de segurança aqui definidos.

BIBLIOGRAFIA

BENETT, Gordon. Intranets: como implantar com sucesso na sua empresa: tradução de ARX Publicações. Rio de Janeiro: Campus, 1997.

BERNSTEIN, Terry. BHIMANI, Anish B. SCHULTZ, Eugene. SIEGEL, Carol A.. Segurança na Internet. Rio de Janeiro: Campus, 1997.

CARVALHO, José Eduardo Maluf de. Introdução às Redes de Computadores. São Paulo: Makron Books, 1998.

HAYDEN, Matt. Aprenda em 24 horas redes: tradução de Marcos Pinto. Rio de Janeiro: Campus, 1999.

JÄHN, Alexandr; AMARAL, Gelson Fernandes do; SIEG, Jacqueline e SANDRIN, Renata. IPSec. [http://inf.unisinos.br/pos-redes/seguranca/ipsec/] (04 de junho de 2001)

MAIA, Luiz Paulo e PAGLIUSI, Paulo Sergio. Criptografia e Certificação Digital. [http://br.geocities.com/jasonbs_1917/seguranca/cripto2.html] (04 junho 2001)

MALAGRINO, Cláudio. Um pouco da história da Internet. [http://www.malagrino.com.br/online/olminter.html] (02 de maio de 2001 14:38)

MARQUES,Alexandre Brandão. Telnet. 1995 [http://www.tche.br/telnet.html] (03 de maio de 2001 17:55)

MORAES NETO, Cyro Mendes de. Como Uma Mensagem É Enviada? 23/12/1999 [http://www.conectiva.com/doc/livros/online/gar/node200.html] 03 de maio de 2001 11:40].

PEREIRA, Aisa. Aprenda Internet Sozinho Agora: História da Internet. [http://www.aisa.com.br/historia.html] (02 de maio de 2001 22:35)

SOARES, Luiz Fernando G.; LEMOS, Guido e COLCHER, Sergio. Redes de computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

SOUZA, Lidenberg Barros de. Redes de Computadores: Dados, Voz e Imagem. São Paulo: Érica, 1999.

SYSTEMS, *Inside Information*. FTP - *File Transfer Protocol*. 1998 [http://www.iis.com.br/info/info_ftp.htm] (03 de maio de 2001 18:22)

TANENBAUM, Andrew S. Redes de computadores. Tradução [ds 3.ed original] Insigth Serviços de Informática. Rio de Janeiro: Campus, 1997.