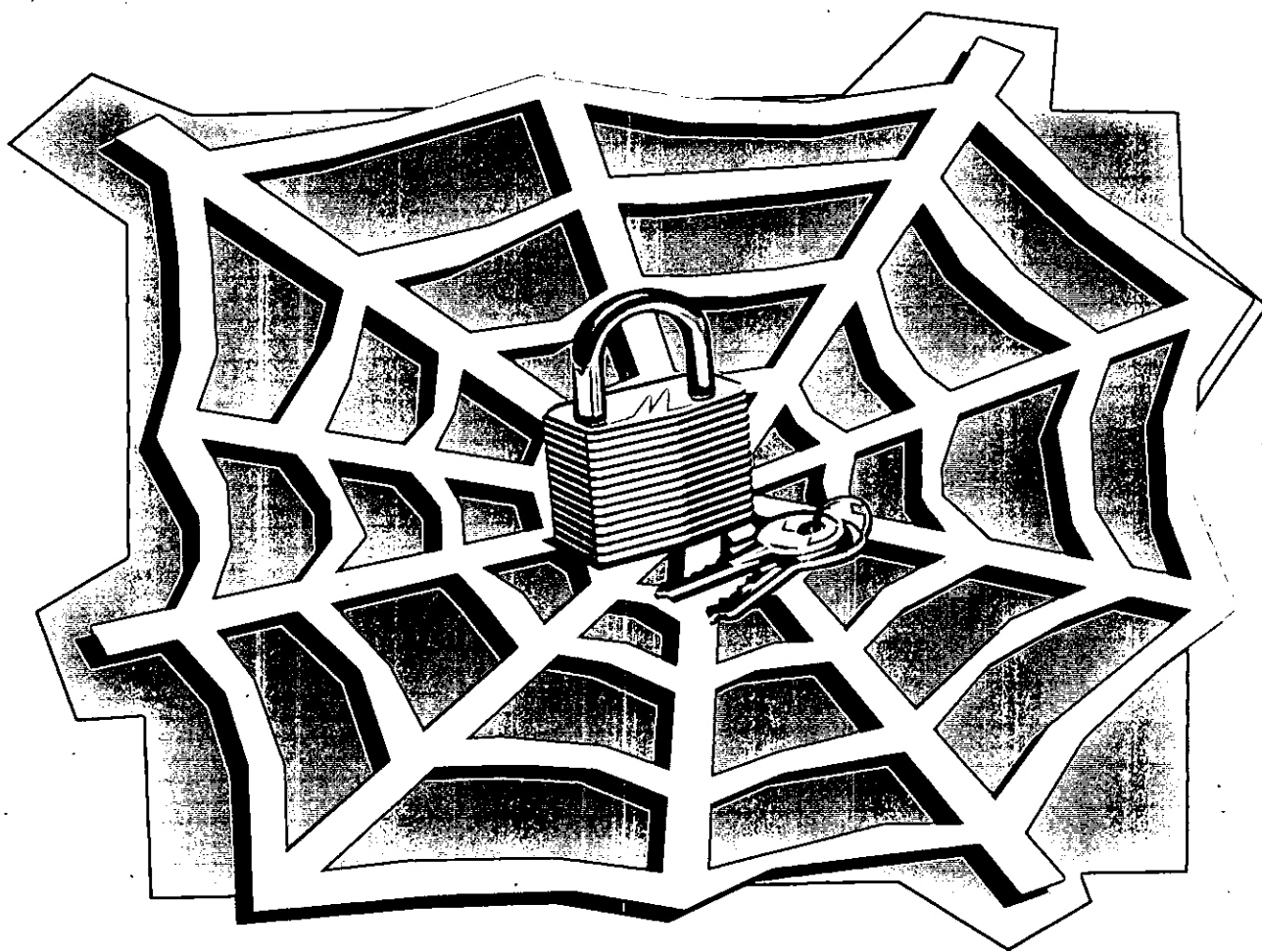


IT-70

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Trabalho de Licenciatura

Modelo de Segurança para o Comércio Electrónico via Internet



Autor: Jorge Teótonio Nhacume

Setembro, 2002.

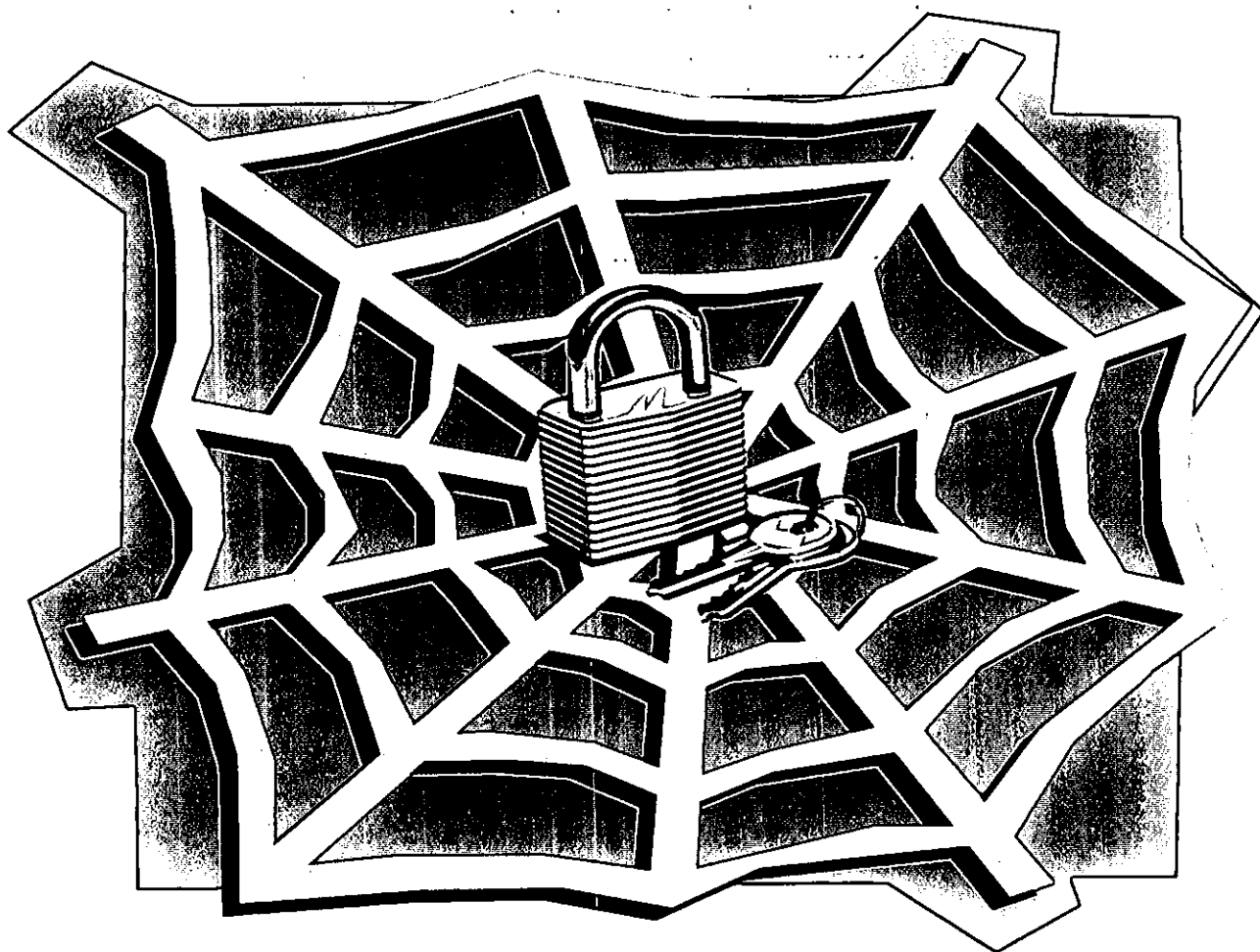
IT-70

IT-70

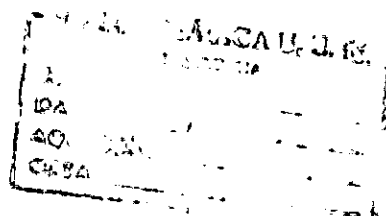
UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Trabalho de Licenciatura

Modelo de Segurança para o Comércio Electrónico via Internet



Autor: Jorge Teótonio Nhacume
Supervisor: dr. Fernando Rafael Comolo



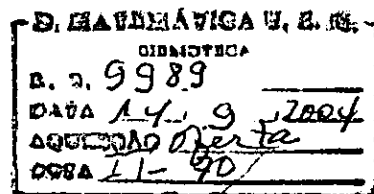
Setembro, 2002.

IT-70

DEDICATÓRIA

Dedico este trabalho ao meu querido pai que não se encontra fisicamente connosco nesta terra, pelos ensinamentos e a minha mãe pelo amor e carinho.

Jorge Teotónio Nhacume



AGRADECIMENTOS

Quero expressar a minha profunda gratidão em especial ao meu supervisor dr. Fernando Rafael Comolo que sem reservas me apoiou para que este trabalho se tornasse realidade, a todos os docentes do DMI que directa ou indirectamente contribuíram para a minha formação académica e para o sucesso do presente trabalho, a minha família e amigos pelo apoio que me deram durante os meus estudos e a Deus que proporcionou que eu chegasse onde estou, e que permanecerá comigo durante as futuras conquistas.

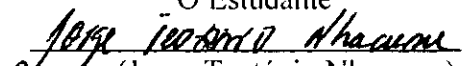
Jorge Teotónio Nhacume.

DECLARAÇÃO DE HONRA

Declaro por minha honra que o presente trabalho constitui resultado das minhas próprias pesquisas e que o mesmo não foi submetido a outro grau que não seja o indicado 'Licenciatura em Informática', na Faculdade de ciências da Universidade Eduardo Mondlane.

Maputo, Setembro de 2002.

O Estudante


(Jorge Teotónio Nhacume)

LISTA DE ACRÓMIOS

CA	Certificate Authority
CE	Comércio Electrónico
CERT	Computer Emergency Response Team
DAT	Digital Audio Tape
DHCP	Dynamic Host Protocol
DMZ	De-Militarized Zone
DNS	Domain Name Service
DoS	Denial of Service
EDI	Electronic Data Interchange
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HTML	Hipertext Markup Language
HTTP	Hipertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering TaskForce
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IRC	Internet Ralay Chat
ISP	Internet Service Provider
LAN	Local Area Netware
NAT	Network Address Translator
NFS	Network File System
NIDS	Network Intrusion Detection System
NIS	Network Information System
POP	Post Office Protocol, Point Of Presence
PPTP	Point To Point Tunneling Protocol
RAS	Remote Access Server
SET	Secure Electronic Transaction
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WWW	World Wide Web

RESUMO

A evolução da Internet tem facilitado extraordinariamente a comunicação entre empresas e pessoas no mundo inteiro, entretanto uma grande preocupação começou a ressurgir nesse ambiente: A Segurança da Informação. Esse é um dos assuntos mais comentados nos meios de tecnologia da informação actualmente.

Os ataques contra sistemas conectados à Internet nos dias de hoje são mais sérios e complexos do que eram no passado. Manter dados, recursos computacionais e principalmente, a reputação da organização protegida se tornou tarefa para profissionais dedicados ao estudo de segurança da informação.

O objectivo deste trabalho é apresentar as ferramentas e medidas para a melhoria da segurança no comércio electrónico via Internet.

Ao longo do trabalho são apresentados os conceitos tecnológicos envolvidos neste processo, as principais técnicas de ataque e ameaças existentes, as vulnerabilidades encontradas na Internet, ferramentas e medidas para garantir a segurança no CE, assim como a proposta de um modelo de segurança de dados que trafegam na rede.

Em função do comportamento da pesquisa são estudados métodos de segurança inéditos para o ambiente de trabalho do CE, mais aprimorados que os actuais, propondo a adição de uma nova camada de segurança nas redes.

O presente trabalho espera também mostrar como a aplicação correcta de técnicas e ferramentas podem trazer benefícios para a segurança do comércio electrónico numa organização.

Conclui-se que o cumprimento das recomendações especificadas neste trabalho auxilia efectivamente na protecção das redes de trabalho, servidores e dados expostos na Internet.

ÍNDICE

CAPÍTULO 1: INTRODUÇÃO E OBJECTIVOS.....	1
1.1. INTRODUÇÃO.....	1
1.2. DEFINIÇÃO DO PROBLEMA.....	1
1.3. IMPORTÂNCIA DO TRABALHO.....	2
1.4. OBJECTIVOS.....	3
1.4.1. Objectivos Gerais.....	3
1.4.2. Objectivos específicos.....	3
CAPÍTULO 2: MATERIAL E MÉTODOS	4
1. COLHEITA DE DADOS.....	4
2. MÉTODO DE ANÁLISE.....	4
3. AVALIAÇÃO DO MODELO PROPOSTO	4
CAPÍTULO 3: CONCEITOS E FUNDAMENTOS	5
1. INTERNET.....	5
1.1. SERVIÇOS DA INTERNET	5
1.1.1. A World Wide Web	5
1.1.2. A Web.....	6
1.1.2.1. Considerações sobre segurança	6
1.1.3. O protocolo HTTP.....	6
1.1.4. A linguagem HTML	6
1.1.5. Correio electrónico	7
1.1.5.1.Considerações sobre segurança	7
1.1.6. Transferência de ficheiros	8
1.1.6.1. Considerações sobre segurança	8
1.1.7. Terminais Remotos(Telnet).....	8
1.1.7.1.Considerações sobre segurança	9
2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO.....	9
2.1. AUTENTICIDADE	9
2.2. CONFIDENCIALIDADE.....	10
2.3. INTEGRIDADE.....	10
2.4. DISPONIBILIDADE.....	10
2.5. NÃO - REPÚDIO.....	11
2.6. CONTROLE DE ACESSO	11
CAPÍTULO 4: COMÉRCIO ELECTRÓNICO	12
1. TIPOS PRINCIPAIS DO COMÉRCIO ELECTRÓNICO	12
2. VANTAGENS DO COMÉRCIO ELECTRÓNICO.....	14
3. MEIOS DE PAGAMENTOS ELECTRÓNICOS.....	14
3.1. Cartão de crédito.....	15
3.2. Cash digital ou electrónico	15
3.3. Cheques Electrónicos.....	16
4. ELECTRONIC DATA INTERCHANGE(EDI)	16
5. IMPACTO DA COMÉRCIO ELECTRÓNICO	16

CAPÍTULO 5: AMEAÇAS, VULNERABILIDADES E TÉCNICAS DE ATAQUE	18
1. TIPOS DE AMEAÇAS.....	18
2. PONTOS VULNERÁVEIS INATOS DA INTERNET	18
2.1. PONTOS FRACOS NA TECNOLOGIA.....	19
2.2. PONTOS FRACOS INERENTES.....	19
2.3. PONTOS FRACOS NA POLÍTICA DE OPERAÇÃO.....	20
2.4. PONTOS FRACOS NA CONFIGURAÇÃO.....	20
3. INTRUSOS.....	21
4. ATAQUES NA INTERNET	21
4.1. SNIFFERS (FAREJADORES)	21
4.2. SPOOFING DE IP.....	22
4.3. DENIAL OF SERVICE (DOS).....	22
4.4. ATAQUE DO TIPO DDOS	22
4.5. ATAQUES BASEADOS EM SENHAS	23
4.6. PORT SCANNING.....	24
4.7. ATAQUES DE VÍRUS.....	24
4.8. TROJAN HORSE(CAVALOS DE TRÓIA).....	24
4.9. BACKDOORS	25
4.10. APPLETS	25
4.11. ENGENHARIA SOCIAL	26
CAPÍTULO 6: MÉTODOS E FERRAMENTAS DE SEGURANÇA.....	27
1. SEGURANÇA FÍSICA.....	27
2. SEGURANÇA LÓGICA	27
2.1. AUTENTICAÇÃO	27
2.1.1. Senhas	28
2.1.2. Smart Cards (Cartões Inteligentes)	28
2.1.3. Biometria	28
2.1.4. On -Time Password	28
2.2. SISTEMAS DE DETECÇÃO DE INTRUSÃO(IDS).....	28
2.3. LOGS E AUDITORIA.....	29
2.4. RECUPERAÇÃO DE DESASTRES E BACKUPS	30
2.5. CRIPTOGRAFIA	30
2.5.1. ALGORITMOS CRIPTOGRÁFICOS	30
2.5.1.1. Algoritmos de chave simétrica ou chave secreta.....	31
2.5.1.2. Algoritmos de chave assimétrica ou chave pública	31
2.5.2. ENVELOPES DIGITAIS	32
2.5.3. ALGORITMOS DE SUMÁRIO.....	33
2.5.4. ASSINATURAS DIGITAIS.....	34
2.5.5. CERTIFICADOS DIGITAIS	35
3. MÉTODOS PARA OBTER SEGURANÇA.....	36
3.1. SSL (Secure Socket Layer).....	36
3.2. SET (Secure Electronic Transaction).....	37
3.3. REDES PRIVADAS VIRTUAIS (VPNS).....	38
3.3.1. PPTP - Point to Point Tunneling Protocol.....	38

4. FIREWALLS	39
4.1. LIMITAÇÕES DE FIREWALLS	41
5. ANTIVÍRUS	41
6. NÍVEIS DE SEGURANÇA.....	42
6.1. O nível de segurança para o comerciante	42
6.2. O nível de segurança para o cliente	42
CAPÍTULO 7: MODELO DE SEGURANÇA PROPOSTO	44
1. MODELO PARA PROTECÇÃO DE REDES	44
1.1. ROTEADOR	45
1.2. BRIDGE HOST	46
1.3. NAT.....	46
1.4. O LOG HOST	48
1.5. AS REDES DE SERVIDORES E WORKSTATIONS.....	48
1.6. REQUISITOS PARA A IMPLEMENTAÇÃO DO MODELO.....	49
1.6.1. HARDWARE	49
1.6.2. SOFTWARE	49
1.6.2.1. O SISTEMA OPERATIVO DO BRIDGE HOST	50
1.6.2.2. DETECTOR DE INTRUSOS.....	50
1.6.2.3. BLOQUEADOR DE ACESSO	51
1.7. VPNS ENTRE OS SERVIDORES.....	51
2. SEGURANÇA NO SERVIDOR DO COMÉRCIO ELECTRÓNICO.....	51
2.1. PROTECÇÃO DE DADOS NO SERVIDOR	52
2.2. ARMAZENAMENTO DE BACKUPS	53
3. AUTENTICAÇÃO.....	53
4. PROTECÇÃO CONTRA VÍRUS E CAVALOS DE TRÓIA.....	53
5. SEGURANÇA FÍSICA	54
6. ATAQUES INTERNOS E ENGENHARIA SOCIAL.....	54
7. GESTÃO DE SERVIDORES	54
8. RESPOSTA A INCIDENTES	55
CAPÍTULO 8: AVALIAÇÃO DO MODELO	56
CAPÍTULO 9: CONCLUSÕES E RECOMENDAÇÕES.....	57
CAPÍTULO 10: BIBLIOGRAFIA	59
1. REFERÊNCIAS BIBLIOGRÁFICAS	59
2. BIBLIOGRAFIA CONSULTADA	60
ANEXOS	I
GLOSSÁRIO.....	A

ÍNDICE DE FIGURAS

Figura 1. Algoritmo de chave simétrica.....	31
Figura 2. Algoritmo de chave assimétrica.....	32
Figura 3. Construção do envelope digital.....	33
Figura 4. Algoritmo de sumário.....	34
Figura 5. Geração de uma assinatura digital.....	34
Figura 6. Verificação de uma assinatura digital.....	35
Figura 7. Restrição de acesso implementada no roteador.....	39
Figura 8. <i>Proxy server</i> intermediando conexões.....	40
Figura 9. Topologia de acesso a Internet com zona desmilitarizada(DMZ).....	40
Figura 10. Segurança no navegador.....	43
Figura 11. Visão geral do modelo proposto.....	45

CAPÍTULO 1: INTRODUÇÃO E OBJECTIVOS

1.1. INTRODUÇÃO

A Internet também chamada auto-estrada da informação pela média conecta computadores espalhados em todo o planeta de uma forma que mesmo os futuristas poderiam supor.

Os serviços fornecidos a utilizadores finais representam apenas alguma parte dos que existem. Por outro lado, estão os serviços oferecidos por empresas e outras organizações conectadas a Internet. A Internet oferece inúmeras oportunidades de negócio, incluindo a divulgação de anúncios publicitários, fabricação e distribuição de produtos e comércio electrónico.

Actualmente, fazer negócio na Internet é o ponto crucial de muitas organizações em vários pontos do mundo. Aproveitar o potencial da Internet é uma tarefa que deveria envolver todas as áreas da organização. Cada área funcional pode contribuir isoladamente ou colectivamente. Por exemplo, o departamento de Marketing, poderá desenvolver as estratégias de propaganda para actividades relacionadas com vendas, talvez criando páginas em servidor de Web. O departamento de vendas poderá criar uma vitrine virtual. Outros departamentos da empresa poderão investigar as possibilidades de uma integração vertical ou horizontal electronicamente facilitada, para seus processos de fabricação.

Novos modelos demográficos significam novas categorias de consumidor, novos mercados virtuais e para simplificar, mais negócios. Recursos e mercados virtuais, juntamente com canais de distribuição global, traduzem-se em infinitas novas possibilidades comerciais. A Internet funciona como um "possibilitador" de negócios facilitando objectivos comerciais - chaves. Todos os sectores da economia podem se beneficiar desta nova tecnologia, tanto o sector de vendas no varejo e no atacado, quanto o sector de serviços financeiros podem ganhar dinheiro com estas novas oportunidades.

1.2. DEFINIÇÃO DO PROBLEMA

Com o crescimento astronómico da Internet, empresas do mundo inteiro vêem inúmeras oportunidades com a chegada desse novo meio de comunicação. Algumas empresas vêem a Internet como uma ferramenta para agilizar os processos mercantis que já existem, outras a consideram como uma forma de oferecer novos serviços e de criar novas fontes de rendimento. Existem prognósticos de que um dia

todas as transações comerciais, desde a prestação de serviços á compra e venda de mercadorias e serviços poderão ser conduzidos na Internet.

Infelizmente, muitas empresas estão se apressando para usar a Internet por motivos comerciais sem considerar as ameaças relacionadas com a segurança necessária nessas conexões. Já se testemunhou centenas de ataques á Internet, sendo que muitos deles foram extremamente sérios. A impossibilidade de concluir controles de segurança adequados para conexões com a Internet pode fazer com que a empresa se torne vulnerável a ataques que poderão deixá-la em situação altamente embaraçosa e causar directrizes para garantir a segurança de informações confidenciais de uma empresa durante a realização das transações comerciais na Internet.

O presente trabalho tem como objectivo não só apresentar as soluções técnicas para controlar a segurança nas transações comerciais efectuadas pelas empresas via Internet como também avaliar as perspectivas comerciais e de gestão sobre como, quando e porquê implementar esses controles, portanto a intenção é tratar das necessidades e preocupações da comunidade ligada a área de negócios.

1.3. IMPORTÂNCIA DO TRABALHO

Este trabalho apresenta uma introdução dos conhecimentos dos riscos que as empresas incorrem ao buscar os seus objectivos comerciais através de conexões com a Internet, bem como fornece abordagens teóricas e práticas sobre os métodos de segurança que são empregues para implementação de segurança no comércio electrónico via Internet.

O desenvolvimento deste trabalho é justificado pela necessidade de protecção das informações que se armazenam e se publicam nos servidores ligados a Internet. Manter a integridade de tais informações requer profissionais adequadamente especializados para esta finalidade, já que se trata de um esforço, para que a aplicação de conceitos de segurança não fique desactualizada sobretudo quando se trata de computadores ligados através de redes.

1.4.OBJECTIVOS

1.4.1. Objectivos Gerais

- Apresentar soluções técnicas para controlar segurança no comércio electrónico via Internet, de forma a minimizar as deficiências existentes na Internet.

1.4.2. Objectivos específicos

- Estudar as transações comerciais via Internet;
- Avaliar os pontos vulneráveis inatos na Internet;
- Avaliar as ameaças à segurança no comércio electrónico via Internet;
- Avaliar as soluções técnicas existentes para controlar segurança do comércio electrónico via Internet;
- Propor um modelo de segurança adequado à perspectiva comercial e de gestão.

CAPÍTULO 2: MATERIAL E MÉTODOS

Para a realização do presente trabalho e a obtenção dos objectivos recorreu-se á:

1. COLHEITA DE DADOS

- Consultas à Internet em sites especializados em CE e segurança de informação;
- Revisão e aprofundamento de conhecimentos adquiridos ao longo da vida académica e profissional através de pesquisas bibliográficas em livros e revistas;
- Entrevistas aos gestores de empresas dedicadas a áreas comerciais;
- Experimentação prática de algumas ferramentas envolvidas.

2. MÉTODO DE ANÁLISE

No presente trabalho foram usadas as metodologia descritiva e comparativa tendo em conta o plano de segurança que contém as acções necessárias para dotar qualquer organização de segurança de informações. Este plano divide-se em fases clássicas (ver ANEXOS I.1.), onde os resultados de uma subsidiam as fases posteriores, formando uma cadeia de acções.

3. AVALIAÇÃO DO MODELO PROPOSTO

A avaliação do modelo proposto foi feita a partir da exposição e entrevistas feitas aos gestores e administradores de redes e sistemas em algumas empresas moçambicanas, com o objectivo de obter informações relevantes em relação aos aspectos de segurança que podem ditar o alcance de resultados satisfatórios após implementação do modelo proposto.

CAPÍTULO 3: CONCEITOS E FUNDAMENTOS

1. INTERNET

A Internet é uma rede pública de comunicação de dados, com controle descentralizado e que utiliza o conjunto de protocolos TCP/IP como base para a estrutura de comunicação e seus serviços de rede. Isto deve-se ao facto de que a arquitectura TCP/IP fornece não somente os protocolos que habilitam a comunicação de dados entre redes, mas também define uma série de aplicações que contribuem para a eficiência e sucesso da arquitectura (Bortoluzzi, 2001).

1.1. SERVIÇOS DA INTERNET

- World Wide Web (HTTP);
- Correio eletrónico (que usa os protocolos SMTP, POP);
- Transferência de ficheiros (FTP);
- Partilha de ficheiros (NFS);
- Acesso a terminal remota (Telnet).

A Internet é dita ser um sistema aberto uma vez que todos os seus serviços básicos assim como as aplicações são definidas publicamente, podendo ser implementadas e utilizadas sem pagamento de licenças para outras instituições.

O conjunto de protocolos TCP/IP foi projectado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte directo a comunicação entre redes de diversos tipos. Neste caso, a arquitectura TCP/IP é independente da infra-estrutura de rede física ou lógica empregada. Qualquer tecnologia de rede pode ser empregue como meio de transporte dos protocolos TCP/IP.

1.1.1. A World Wide Web

Actualmente, o serviço de *world wide web* é um dos mais populares da Internet. Para que se entenda claramente do que é composta esta grande porção da rede pode ser dividida nas seguintes estruturas:

- O protocolo http (hypertext transfer protocol);

- A linguagem HTML (hypertext markup language);
- Os navegadores (Browsers).

1.1.2. A Web

Consiste na colecção de servidores na Internet que atendem a requisições no protocolo de comunicação HTTP. É baseado em conceitos desenvolvidos na *European Particle Physics Laboratory* (CERN) em Genebra, na Suíça, por Tim Berners-Lee e outros pesquisadores. Hoje, muitas organizações e indivíduos estão desenvolvendo este serviço da rede e um número muito maior de empresas e pessoas estão fazendo uso desta tecnologia. A *Internet Engineering TaskForce* (IETF) é responsável por manter o HTTP padronizado e o *World Wide Web Consortium*(W3C) por desenvolver seus futuros sucessores.

1.1.2.1. Considerações sobre segurança

Quando se mantém um servidor da *Web*, se permite que qualquer pessoa o alcance e envie comandos para ele. Os riscos de segurança se encontram quando o *software* servidor deixa de somente manipular HTML para chamar acesso a programas ou módulos externos que ampliam as suas capacidades. Estes programas são relativamente fáceis de se escrever porém difíceis de se implementar porque não se consegue prever todas as passagens de comandos que poderá receber e o comportamento que terá em sua execução.

1.1.3. O protocolo HTTP

É um dos protocolos que fazem parte da camada de aplicação do TCP/IP. Provê aos utilizadores acesso a ficheiros que fazem a *Web*. Estes podem ter diferentes formatos (texto, gráficos, audio, vídeo etc.) mas primariamente ligados através de *hyperlinks* e programados na notação *HTML*.

1.1.4. A linguagem HTML

É uma linguagem de descrição padronizada para criação de páginas na WWW. Basicamente, provê capacidades de formatação de documentos, introdução de imagens, formulários, alteração de fontes, etc. e referência à outros documentos através dos *hyperlinks* (Bortoluzzi, 2001).

1.1.5. Correio electrónico

O Correio Electrónico ainda é um dos serviços mais usados na Internet. Esse serviço tornou-se rapidamente num requisito fundamental para a comunicação comercial. Quando inicialmente desenvolvido, tinha como objectivo funcionar como uma ferramenta para que as pessoas se comunicassem. Com o crescimento da Internet, a comunicação electrónica mudou muito. Várias empresas usam correio electrónico como uma forma de comunicação comercial regular e até como parte de importantes processos, pois trata-se de um serviço relativamente de baixo custo (Bortoluzzi, 2001).

O SMTP é o protocolo padrão na Internet para o transporte das mensagens entre computadores. A exemplo de quase todos os outros serviços da Internet, o correio electrónico não foi definido tendo segurança em mente (Bortoluzzi, 2001).

Várias soluções têm sido analisadas com respeito à segurança do correio electrónico. Embora todas elas utilizem técnicas de criptografia de chave pública, variam da maneira como implementam a tecnologia, precisam de enfrentar questões como, por exemplo, recuperação, revogação e armazenamento de certificados (Bortoluzzi, 2001).

1.1.5.1. Considerações sobre segurança

Servir correio eletrônico toma espaço em disco e tempo de processamento no host, ficando aberto para ataques de negação de serviço e muitas vezes deixa-se um canal aberto para a entrada de cavalos de Tróia. Também é comum neste sistema o envio em massa de mensagens não solicitadas, bem como a confiança exagerada que as pessoas têm no serviço, fazendo seu uso para envio de informações confidenciais sem o mínimo de preocupação com os intermediadores entre o remetente e o destinatário (Bortoluzzi, 2001).

POP e IMAP têm as mesmas implicações de segurança, eles comumente transferem as informações de autenticação do utilizador sem nenhum recurso de criptografia, permitindo a *hackers* lerem tanto suas credenciais quanto as mensagens que estão para ser transmitidas (Bortoluzzi, 2001).

1.1.6. Transferência de ficheiros

FTP é o serviço padronizado na Internet para transferência de ficheiros. A maioria dos navegadores baseados no protocolo HTTP também implementam este protocolo como uma extensão dos seus recursos.

1.1.6.1. Considerações sobre segurança

A primeira preocupação em servir o protocolo FTP é que ele pode actuar como ponto de entrada para cavalos de Tróia e outros códigos maliciosos que exploram falhas na implementação deste serviço. Outras vezes o motivo da preocupação é sobre o licenciamento do conteúdo que é enviado para o servidor. Entre eles, softwares comerciais, jogos copiados ilegalmente e conteúdo pornográfico. Apesar de não apresentarem um risco técnico de segurança, este conteúdo implica em vários outros problemas relevantes, como distribuição ilegal de *software* e infracções fiscais.

1.1.7. Terminais Remotos(Telnet)

Há muitas situações em que é necessário ou ao menos, desejável, executar comandos em computadores diferentes daquele que se está fazendo uso. Muitas vezes o motivo que justifica esta necessidade é o facto de se estar fisicamente muito distante do computador a controlar. Como solução, implementou-se serviços capazes de prover esta tarefa, tanto em computadores com sistema operativo orientado ao modo texto quanto nos que utilizam interfaces gráficas.

Telnet está, cada vez mais, deixando de ser o serviço padronizado na Internet para tarefas de administração remota. Porém, este serviço já foi considerado seguro por requerer credenciais do utilizador. Entretanto, estas credenciais podem ser tão facilmente capturadas através da rede que seu uso se torna muito arriscado (Bortoluzzi, 2001)

Para solucionar as sérias falhas do Telnet, criou-se o tão bem aceite SSH, que provê uma colecção de utilitários capazes de fornecer serviços criptografados de execução remota de comandos, como também, transferência segura de ficheiros. Implementações deste protocolo estão disponíveis através de vários fornecedores e estão se tornando o novo padrão no que diz respeito à administração remota.

1.1.7.1. Considerações sobre segurança

Na utilização do SSH de forma a evitar o uso indevido deste serviço, recomenda-se o seguinte (Bortoluzzi, 2001):

- Explorar ao máximo as capacidades inovadoras para autenticação do utilizador. Isto significa exigir mais que apenas o par login e senha. Como recurso embutido, as implementações SSH podem ser configuradas para exigir uma chave pública do utilizador que tenha sido gerada por uma chave privada anteriormente instalada no servidor. Este procedimento faz com que o utilizador não só forneça algo que só ele tenha conhecimento (senha) mas também algo que somente ele possua (o par de chaves criptográficas).
- Quando financeiramente viável, exigir identificação através de recursos menos quebráveis ainda, como autenticação por *SmartCards*, que armazenam a chave pública do utilizador e são praticamente impossíveis de se forjar.

2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação busca reduzir os riscos de fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou uma organização. Segundo (Silva et al, 1999) uma solução de segurança adequada deve satisfazer os seguintes princípios:

2.1. AUTENTICIDADE

O controle de autenticidade está associado a identificação correcta de um utilizador ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isto é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um utilizador para um sistema, de um sistema para o utilizador ou de um sistema para outro sistema. Ela é a medida de protecção de um serviço/informação contra a personalização por intrusos.

2.2. CONFIDENCIALIDADE

É frequente uma empresa deter uma posição privilegiada em relação a um determinado mercado ou cliente, por estar na posse de determinadas informações, desconhecidas pelos seus concorrentes. Deste modo, é natural que concentre uma parte das suas forças na tentativa de manter essas informações em segredo. Todas as operações que a empresa realiza e que envolvam o uso ou transmissão de informações sensíveis são feitas com maior cautela, como forma de manter a confidencialidade.

A confidencialidade pode ser obtida, essencialmente, através da codificação da informação que se pretende transmitir, de modo que apenas o destinatário tenha acesso a essa informação.

2.3. INTEGRIDADE

Se por exemplo, um comprador faz uma encomenda de uma certa quantidade de um produto a um fornecedor, é de esperar que este receba os dados da encomenda na forma original. Se sofrerem alguma modificação quando transitam do emissor para o receptor(em termos de quantidade), obviamente, este vai receber uma encomenda que não têm nada a ver com as intenções iniciais do emissor.

A modificação referenciada pode ser de origem accidental ou maliciosa. Em ambos os casos, é conveniente evitar que este tipo de situações sejam possíveis logo à partida. Neste caso, o fornecedor deverá ter mecanismos necessários para verificação da integridade da encomenda recebida, isto é, que o conteúdo desta coincide com o enviado pelo comprador.

Porém, a garantia de integridade de dados não impede que estes sofram modificações antes de chegarem ao destino final. No entanto se estas modificações ocorrerem, facilmente podem ser detectadas pelo receptor. No caso da encomenda o fornecedor não aceitaria a encomenda.

2.4. DISPONIBILIDADE

Diz respeito à necessidade de se ter informações acessíveis e prontas para o uso, o que representa um objectivo crítico para qualquer empresa que se baseia no processamento de computadores. Sem sistemas de segurança que utilizam esses controles, uma empresa não pode ter garantia de segurança.

Outros princípios:

2.5. NÃO - REPÚDIO

Se for importante que um interlocutor possa ter a certeza sobre a identidade e poderes de um seu parceiro numa transação, não é menos importante que nenhum dos parceiros seja capaz de negar a sua participação nessa transacção. A esse tipo de garantia dá-se o nome de não-repúdio.

2.6. CONTROLE DE ACESSO

É a habilidade de limitar ou controlar o acesso aos computadores ou aplicações através de enlaces de comunicação e controlo de acesso físico.

CAPÍTULO 4: COMÉRCIO ELECTRÓNICO

O comércio é uma actividade inerente ao ser humano. Desde tempos longínquos que a troca e compra de bens ou serviços faz parte do quotidiano do homem. Actualmente, na época de globalização e da informação, o comércio electrónico veio acelerar consideravelmente os processos de negócios das empresas, rentabilizar os seus recursos humanos e promover novos modelos de negócio e paradigmas de interacção entre empresas e entre estas e consumidores finais.

Assim define-se o comércio electrónico com sendo qualquer sistema tecnológico e económico que potencia ou facilita a actividade comercial e um conjunto variado de participantes através de mecanismos electrónicos (Silva et al, 1999).

Segundo (Silva et al, 1999) o CE; Compra e venda de mercadorias e serviços através de um meio electrónico será das mais importantes maneiras de fazer negócio no futuro.

Nos últimos tempos, porém o progresso tem sido mais lento devido a falta de mecanismos seguros para efectuar pagamentos electronicamente na Internet.

O CE é a nova fronteira, e como tal, tem a sua própria linguagem e terminologia. Primeiro existem instrumentos financeiros associados ao CE, tais como o *dinheiro electrónico (dinheiro digital)*, *cartões de crédito*, *cartões inteligentes (smart cards)* e *cheques electrónicos*. Segundo há muitos termos de contabilidade usados para descrever os diferentes tipos de sistemas de pagamento electrónico: *pagamento anónimo*, *pagamento identificado*, *sistemas On-line*, *sistemas Off-line*, *transacções "às cegas"*. Por último, existem as tecnologias que activam a segurança: *Criptografia com chave pública*, *assinatura digital*, *autenticação*, *credenciais e certificados digitais*. Todos esses termos são conhecidos dos que projectam e implementam sistemas de pagamentos seguros.

1. TIPOS PRINCIPAIS DO COMÉRCIO ELECTRÓNICO

Segundo (Ferrão, 2000) o CE pode assumir várias formas no contexto dos relacionamentos entre várias entidades; Os clientes, as empresas, as organizações em geral e a própria administração pública:

- *Business to Business* (entre empresas) ou B2B: Trata-se do relacionamento entre empresas normalmente para o caso de empresas - clientes e empresas - fornecedoras de produtos/serviços.

Em vários casos ter-se-á mesmo a implementação de uma rede informática, que no caso actual poderá ser uma Extranet em que as interações se procuram fazer de forma automática. Este tipo de relacionamento foi dos primeiros a ser implementado no CE, com a adopção do EDI como suporte de troca de documentos com a Internet, hoje em dia o B2B aplica-se também ao caso de ligações de uma empresa com seus canais de distribuição, procurando-se assim uma maior rapidez na satisfação das encomendas dos clientes finais, ou mesmo para atendimento das reclamações.

- *Business to Consumer* (Empresas - Clientes finais): Neste caso podemos dizer que temos uma “venda a retalho electrónico”, ou seja, com grande desenvolvimento da Internet, foi possível estender aos clientes individuais, o tipo de relacionamento que tinha anteriormente apenas com empresas. A variedade de formas que o CE tem vindo a ter em conta neste caso excede em muito apenas as trocas comerciais e as formas de comercialização. Com efeito existem hoje na Internet as chamadas “Lojas Virtuais” a semelhança das que existe na vida real. Para além disso é também possível a compra de produtos/serviços novos que só podem ser comercializados através da Internet.
- *Within Business* (dentro das empresas): Destina-se essencialmente a promover a troca/divulgação de informação dentro de empresas através neste caso da Internet, ou redes do tipo Intranet instaladas nas empresas. Neste caso teremos a comunicação entre vários grupos funcionais que constituem a empresa tal como no caso das interações entre clientes, como no caso anterior. Por outro lado poderá ser usado também para a difusão de informação em geral tal como documentos técnicos, manuais, informação referente aos recursos humanos ou mesmo comercial (locais de venda, lista de revendedores, etc.)
- *Business - Administration* (Empresa - Governo): Para cobrir todas as transações possíveis entre as empresas e as várias instâncias governamentais. Neste momento, ainda no seu início, poderá vir a ter um grande desenvolvimento no futuro, em termos de não só aspectos legais, formalidades a cumprir, mas também no que diz respeito a compras na administração pública.
- *Consumer - Administration* (Cliente/Cidadão - Governo): Esta é uma forma relacionada que já foi iniciada com possibilidade e entrega de declarações impostos através da Internet. Será com certeza uma forma de CE com grandes perspectivas de evolução futura, desde que se garantam

as necessárias condições de segurança da informação, que poderá mesmo estender-se a administração local para o relacionamento cidadão - autarquia.

2. VANTAGENS DO COMÉRCIO ELECTRÓNICO

Segundo (Ferrão, 2000) entrar em negócios electrónicos tem muitas vantagens:

- *Acessibilidade global e alcance de vendas:* Empresas podem expandir sua linha de clientes e até mesmo sua linha de produtos.
- *Relacionamento mais próximo:* Transação business-to-business podem gerar relações mais próximas.
- *Testes gratuitos:* Produtos podem ser testados na Web de forma mais rápida, fácil e sem custos.
- *Custos reduzidos:* As empresas podem reduzir seus custos de produção adequando dinamicamente os preços.
- *Mudança de meios de comunicação:* A Internet reduz o número de mudanças de meios de comunicação necessárias para transportar a informação.
- *Tempo para comercialização:* Tempo mais curto para comercializar e menor tempo de resposta em relação às mudanças de demanda do mercado.
- *Lealdade de clientes:* Melhoria na lealdade dos clientes e nos serviços por meio de acessos mais fáceis a informações actualizadas e sempre disponível.

3. MEIOS DE PAGAMENTOS ELECTRÓNICOS

Em qualquer actividade comercial há geralmente uma troca de valores entre os participantes, dividindo estes simplesmente por vendedores e compradores, têm-se que os primeiros fornecem produtos/serviços e os segundos retribuem com uma forma de pagamento que em última análise representa um valor que o vendedor considera equivalente ao produto/serviço.

Esta realidade não se altera quando se pensa em CE na Internet, também aí os vendedores querem ser pagos pelos produtos ou serviços que disponibilizam. Por seu turno, os compradores querem garantia que não pagam mais do que aquilo que estão a espera. Portanto, a informação que enviam aos vendedores não deve poder ser utilizada por outra pessoa para realizar pagamentos em seu nome.

Existem outros requisitos, dos quais destaca-se a privacidade em relação aos dados pessoais e bens adquiridos, informação esta que pode ser disponibilizada quando se efectuam pagamentos. Segundo (Albertini, 2000) os meios de pagamentos mais utilizados são:

3.1. Cartão de crédito

É um serviço de intermediação que permite ao consumidor adquirir bens e serviços em estabelecimentos comerciais previamente credenciados mediante a comprovação de sua condição de utilizador. Essa comprovação é geralmente realizada, no acto da aquisição, com a apresentação de cartão ao estabelecimento comercial. O cartão é emitido pelo prestador do serviço de intermediação, chamado de administradora de cartão de crédito, que pode ser um banco. O estabelecimento comercial registra a transação com o uso de máquinas mecânicas ou informatizadas, fornecidas pela administradora do cartão de crédito, gerando um débito do consumidor a favor da administradora e um crédito do fornecedor do bem ou serviço contra a administradora, de acordo com os contratos firmados entre estas partes. Periodicamente, a administradora do cartão emite e apresenta a factura ao consumidor, com a relação e o valor das compras efectuadas.

A administradora, de acordo com o contrato firmado com o consumidor, fica responsável pelo pagamento das aquisições feitas por ele com o uso do cartão, até um valor limite combinado. A administradora, também de acordo com o contrato firmado com o fornecedor de bens e serviços, fica responsável, directamente ou por meio de empresa especializada, pelo pagamento das aquisições efectuadas pelo utilizador do cartão.

A relação entre o consumidor e o fornecedor não se altera pela forma de pagamento, sendo mantida a característica de um contrato, escrito ou não, de compra e venda ou de prestação de serviços.

3.2. Cash digital ou electrónico

Também chamado e-cash, se refere a quaisquer meios que permitem uma pessoa pagar bens ou serviços transmitindo um número de um computador para outro. Os números são como uma nota de dinheiro, são emitidos por um banco e representam somas específicas de dinheiro real. Uma das características-chaves de dinheiro digital é que é anónimo e reutilizável, igual a dinheiro real. Esta é uma diferença-chave entre e-cash e transações de cartão de crédito na Internet.

3.3. Cheques Electrónicos

Ainda na fase de teste, retiram dinheiro das contas correntes dos utilizadores para pagar serviços e contas telefónicas.

4. ELECTRONIC DATA INTERCHANGE (EDI)- INTERCÂMBIO DE DADOS ELECTRÓNICOS

Criado pelo governo dos EUA nos anos 70, é uma estrutura de documentos comum projectada para deixar grandes organizações transmitirem informações através de redes privadas. No CE via Internet tem papel importante, pois contém um conjunto de procedimentos que permite as empresas trocarem informações, com avançados recursos de segurança e alto controle sobre a troca de pedidos e informações. Dependendo do volume de transações e do próprio tamanho das empresas, muitas vezes o investimento de se implementar um sistema EDI pleno pode ser alto. Com a Web, surgiram serviços que permitem que as empresas, através da Web, se comuniquem com outras empresas usando o padrão de comunicação do EDI.

Evidentemente, por a alternativa de conectividade via Internet ser mais barata que o EDI tradicional, muitas empresas têm decidido integrar seus processos com outras empresas daquela forma. Entretanto é importante ressaltar que grandes empresas, que usam serviços EDI em larga escala, tendem se manter, pelo menos por algum tempo, com serviços, até porque os padrões da troca de dados via Internet ainda não são tão robustos como EDI (Veloso, 2002).

5. IMPACTO DA COMÉRCIO ELECTRÓNICO

Não há dúvidas que o CE, a exemplo da popularidade da Internet, está causando um grande impacto nos serviços fornecidos pelas instituições financeiras. Nenhuma instituição financeira deixará de ser afectada directa ou indirectamente pela explosão do CE. O número de compras com cartão de crédito realizadas através deste meio está a crescer com os pedidos online dos sistemas baseados na Internet.

Segundo (Veloso, 2002) vários bancos estão planeando aderir a esta nova forma de CE oferecendo autorizações para pagamentos com cartões de crédito directamente pela Internet.

Os sistemas de pagamento e suas instituições financeiras têm uma função significativa estabelecendo especificações abertas para transações com pagamentos em cartão que:

- *Proporcionam transmissões confidenciais:* Para facilitar e encorajar o CE usando os produtos com pagamento em cartão, é necessário garantir aos portadores de cartão que as suas informações de pagamento estão seguras e somente podem ser acedidas pelo destinatário. Portanto, a conta dos portadores de cartão e as informações de pagamento devem ser asseguradas em suas viagens pela rede, prevenindo a interceptação das números das contas e suas datas de expiração por indivíduos não autorizadas.
- *Autenticam as partes envolvidas:* Os comerciantes precisam de uma maneira para verificar que um portador de um cartão é o legítimo utilizador da conta do cartão. Um mecanismo que usa tecnologia para ligar um portador de cartão a um número de uma conta de pagamento de um cartão específico reduzirá a incidência de fraude e conseqüentemente o custo global do processamento do pagamento.
- *Garantem a integridade das instruções de pagamento para bens e serviços:* A informação de pagamento enviada dos portadores de cartão para os comerciantes inclui a informação do pedido, os dados pessoais, e as instruções de pagamento. Se qualquer componente for alterado na transição, a transação não será processada correctamente. Os protocolos de pagamento seguros devem garantir que o conteúdo de cada pedido e a mensagem de pagamento recebida correspondem ao conteúdo da mensagem enviada.
- *Autenticam a identidade do portador do cartão e do vendedor mutuamente:* A especificação deve proporcionar uma maneira para o portador de cartão confirmar que o comerciante possui um relacionamento com uma instituição financeira que o permite aceitar pagamentos em cartão. Os portadores de cartão também precisam estar aptos a identificar os comerciantes com os quais ele pode conduzir seguramente o CE.

CAPÍTULO 5: AMEAÇAS, VULNERABILIDADES E TÉCNICAS DE ATAQUE

Como se vê a Internet pode oferecer grande economia de custos e excelentes ganhos de produtividade, além de oportunidades significativas para geração de receita. Mas para obter esses benefícios as empresas devem expor suas redes a ameaças de segurança potencialmente sérias. Para que se certifique se o património duma empresa está seguro, ela deve compreender essas ameaças e tomar providências necessárias para proteger informações, recursos e redes.

Segundo (Bernstein et al, 1997) as ameaças vêm tanto da Internet quanto de redes internas, mas não na mesma proporção. Significativamente há mais ameaças por parte das redes internas de uma empresa - 80 a 95% do número total de incidentes de segurança. Com isso, obviamente, apenas uma pequena percentagem de ameaças realmente tem origem na própria Internet.

Para garantir a protecção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos intrusos, para então aplicar as medidas e ferramentas necessárias para a protecção desses recursos.

Sem o conhecimento desses factores, toda a aplicação de mecanismos de protecção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorrecta, todo o sistema estará comprometido.

1. TIPOS DE AMEAÇAS

- Ameaça á rede corporativa;
- Ameaça aos servidores da Internet;
- Ameaça a transmissão de dados;
- Ameaça a disponibilidade de serviços;
- Ameaça a repúdio.

2. PONTOS VULNERÁVEIS INATOS DA INTERNET

As ameaças exploram os pontos fracos de um sistema, geralmente relacionados à tecnologia ou a política de operação. As fraquezas tecnológicas se referem a deficiências nos produtos de Software e Hardware que se utiliza assim como as falhas no material de comunicação.

As propriedades intrínsecas da Internet representam a principal fonte da sua vulnerabilidade a falhas e ataques. A Internet conecta antenas de redes regionais e redes de provedores de serviços regionais espalhados pelo mundo inteiro.

A Internet é uma rede pública onde os pacotes trafegam por rotas que não são bem controladas quanto nas redes privadas; Pois, pode haver perda de informações; Talvez os sistemas não estejam sempre funcionando de modo adequado, pessoas ocultas podem conduzir actos de espionagem ou ataques de falsificação ideológica a partir de locais remotos. Protocolos, que definem as regras para o controle de como as mensagens são trocadas em uma rede de computadores, podem apresentar defeitos ou parar de funcionar. Todos estes factores contribuem para que a Internet seja um meio de comunicação não confiável e inseguro.

2.1. PONTOS FRACOS NA TECNOLOGIA

Uma vez que tenham obtido acesso a rede os intrusos podem explorar suas fraquezas. Os *hackers* têm total conhecimento de determinados pontos vulneráveis dos sistemas. Na verdade, com frequência o fornecedor ou o *hacker* divulga a existência de um *bug* do sistema ou de um furo na segurança depois que o problema é descoberto. Organizações como a CERT divulgam pontos vulneráveis (e correcções), jornais informativos destacam os feitos dos *hackers*. A violação de esquemas de segurança é uma novidade, especialmente se estiver relacionada à Internet. Geralmente as fraquezas tecnológicas podem ser classificadas de duas categorias: as causadas por deficiências inerentes a mecanismos e produtos e as que resultam da configuração incorrecta de sistemas operativos e programas de aplicação.

2.2. PONTOS FRACOS INERENTES

Muitos desses problemas podem ser resultantes de deficiências nos protocolos de comunicação. Os protocolos definem o conjunto de regras em que se baseia a inter-operação das redes. Muitos protocolos são usados juntamente com outros e agregados em "*conjunto de protocolos*". O *TCP/IP* é conjunto de protocolos mais comuns na Internet. Infelizmente muitos protocolos *TCP/IP*, têm características inatas que os tornam vulneráveis a ataques, dentre esses problemas podemos destacar (Bernstein et al, 1997):

- Inabilidade para confirmar a identidade dos participantes num processo de comunicação. Sob o *TCP/IP* qualquer computador pode criar mensagens que parecem ter outra origem.

- Inabilidade de proteger a privacidade de dados de uma rede. Devido a uma característica de um dos protocolos TCP/IP básicos uma determinada máquina pode monitorar todo o tráfego de uma rede a que está conectada, independentemente do seu destino.

Essas falhas comprometem os serviços de aplicação, por exemplo, a falta de confidencialidade pode levar ao roubo de logins e senhas do utilizador durante uma transferência de *FTP*.

Os hackers exploram muitos pontos vulneráveis encontrados em protocolos de rede. Geralmente, só se descobre este tipo de “furo” depois de o sistema estar comprometido.

2.3. PONTOS FRACOS NA POLÍTICA DE OPERAÇÃO

As políticas de segurança corporativas estabelecem as bases para um bom modelo de segurança. Essas políticas, frequentemente chamadas controles básicos, funcionam juntos no estabelecimento de um determinado nível de segurança na empresa como um todo. Os controles básicos abrangem (Bernstein et al, 1997):

- Controlo de acesso físico;
- Controle de acesso lógico;
- Administração de segurança;
- Monitoração e auditoria de segurança;
- Gestão de modificações em Software e Hardware;
- Backups e recuperação de desastre;
- Continuidade dos negócios.

Cada um destes controles deve ser implementado de forma consistente, de plataforma para plataforma, em toda a empresa. Nenhuma ligação fraca deve permanecer. Esses controles básicos são essenciais para ajudar a proteger uma rede tanto das ameaças baseadas na Internet como ameaças internas.

2.4. PONTOS FRACOS NA CONFIGURAÇÃO

Para (Bernstein et al, 1997) outro tipo de deficiência decorre pelo facto de que muitos sistemas são grandes, complicados e difíceis de configurar. Muitos sistemas são fornecidos com parâmetros básicos inerentemente inseguros. Alguns exemplos de pontos fracos de configuração de sistemas:

- Contas de utilizadores inseguras (como logins de Guests ou contas expiradas);

- Contas de sistemas com senhas originais muito conhecidos que não são alteradas;
- Serviços de Internet incorrectamente configurados;
- Parâmetros básicos inseguros.

3. INTRUSOS

Durante anos, os profissionais da área de segurança de informações e comunidade que impõe leis tem tentado identificar quem são exactamente os intrusos. Identificar um intruso é uma operação onerosa - mas importante (Bernstein et al, 1997). Uma melhor compressão de quem pode ser o intruso ajuda a prever não só quem tem mais possibilidades de cometer crimes decorrentes de mau uso do computador, como também o que essa pessoa poderá fazer. Identificar os inúmeros motivos que levam pessoas a atacar sistemas de computador é um aspecto muito importante. *Crackers* assumidos revelam os seguintes motivos nos seus actos: *Ganhos financeiros, vingança, necessidade de aceitação ou respeito, idealismo, curiosidade ou busca de emoção, aprendizado, ignorância, espionagem comercial, etc.*

Diante disto é difícil identificar realmente quem é o intruso, os vários tipos de intrusos são motivados por diversos factores. Essa realidade torna a tarefa de proteger sistemas conectados a Internet mais difícil de ser executada. Com frequência, a diversidade de possíveis ataques provocados por variedade de motivos exige o uso de maior número de controles do que o normal.

4. ATAQUES NA INTERNET

Após a discussão dos motivos que levam as pessoas a tentar violar sistemas de computador segue-se a análise das formas mais comuns em que os ataques se manifestam. Apesar de determinados ataques, como o "*spoofing de endereços*" terem recebido muita atenção, é importante lembrar que eles representam apenas alguns dos muitos que já foram observados na Internet.

4.1. SNIFFERS (FAREJADORES)

Por padrão os computadores pertencentes a mesma rede recebem e respondem somente os pacotes endereçados a eles. Entretanto, é possível utilizar um software que coloca a interface num estado chamado promíscuo. Nessa condição o computador pode monitorar e capturar os dados que trafegam na rede, para um destino omisso.

Os programas que capturam os pacotes de rede são chamados sniffers. Eles exploram o facto de o tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados, podendo obter nomes de utilizadores, senhas ou qualquer outra informação transmitida que não esteja criptografada (Medeiros, 2001).

Para se concretizar este tipo de ataque o atacante instala o programa em algum ponto estratégico da rede, como entre duas máquinas (cujo tráfego entre elas passa pela máquina com farejador) ou em uma rede local com interface de rede em modo promíscuo.

4.2. SPOOFING DE IP

É a técnica de se fazer passar por outro computador da rede para conseguir acesso ao sistema. Apesar de spoofing poder ocorrer com diversos protocolos específicos, o spoofing do IP é o mais conhecido dentre todos os ataques spoofing (Bernstein et al, 1997).

Os computadores na Internet são identificados por endereço IP, que são únicos por toda a rede. O IP spoofing é um mecanismo que age directamente na comunicação entre os computadores. Durante a comunicação entre dois computadores (A e B), pode se tirar um deles da acção, neste caso o (B), e utilizar um terceiro computador violador (X) como se fosse B. Isso acontece através de envio de pacotes para o computador (B) por (X) até que ele seja desconectado da rede. Assim o computador (X) assume o endereço IP do computador (B), e continua com a comunicação com o computador A como se fosse original (B).

A melhor defesa contra o spoofing é configurar roteadores de modo a rejeitar qualquer pacote recebido cuja origem alegada seja um host da rede interna. Essa simples precaução impedirá que qualquer máquina externa tire vantagem de relacionamentos confiáveis dentro da rede interna.

4.3. DENIAL OF SERVICE (DoS)

Estes ataques designam-se ataques de negação de serviço, em que o acesso ao sistema/aplicação é interrompido ou impedido, deixando de estar disponível, ou uma aplicação cujo tempo de execução é crítico, é atrasada ou abortada (Medeiros, 2001).

Este tipo de ataque consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços; O intruso invade muitos computadores e instala neles um software

denominado *zumbi* que quando recebem a ordem de iniciar o ataque “disparam” as solicitações ao computador alvo. É um ataque mais fácil de implementar, mas difícil de se evitar (Medeiros, 2001).

O objectivo é incapacitar um servidor, uma workstation ou um sistema de fornecer os seus serviços para os utilizadores legítimos. Este ataque não permite o acesso ou modificação dos dados, geralmente o atacante somente inviabiliza o uso de um serviço (Medeiros, 2001).

Estes ataques não causam a perda ou roubo de informação, apenas atacam o conceito da disponibilidade.

4.4. ATAQUE DO TIPO DDoS

São ataques semelhantes ao DoS, tendo como origem diversos ou até milhares de pontos disparando ataques DoS para um ou mais sites determinados. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes ao serem executados se transformam em um ataque DoS de grande escala.

4.5. ATAQUES BASEADOS EM SENHAS

Esse tipo de ataque envolve alguma forma de exploração de senhas. Uma infiltração de senha comum é aquela em que o intruso informa uma combinação de nome do utilizador/senha, depois outra e assim por diante, até que uma determinada combinação permita a sua entrada no sistema.

Essa estratégia tem sucesso em muitos tipos de sistemas operativos que não bloqueiam tentativas de *Login* após um determinado número de insucessos. Essa fraqueza inerente permite que um intruso dê início a um grande número de tentativas de logins que não são impedidas.

Às vezes, os intrusos descobrem as senhas das seguintes formas: acedendo mensagens de correios electrónicos que contêm senhas, ou decifrando-as com uma ferramenta que permite localizar e obter informações sobre senhas vulneráveis em sistemas UNIX (Bernstein et al, 1997).

4.6. PORT SCANNING

Segundo (Medeiros, 2001) Port scanning é o processo de verificação de quais serviços estão activos num determinado host. As ferramentas de Port Scanning podem verificar redes inteiras, apontando quais hosts estão activos e quais são os seus serviços de rede em funcionamento. Além disso, as ferramentas mais modernas inclusive podem informar qual é o sistema operativo do host verificado.

Sabendo quais são os serviços disponiveis e qual é o sistema operativo, os hackers podem buscar as vulnerabilidades nesses sistemas. Para realizar trabalho obscuro muitas ferramentas Port Scanning utilizam técnicas como Spoofing para ocultar a origem da acção.

4.7. ATAQUES DE VÍRUS

Um ataque de vírus pode ser muito prejudicial para qualquer computador, e principalmente para a rede da empresa formada por muitos computadores. (Medeiros, 2001) define vírus como sendo pequenos programas que se “colam” a outros e se copiam a si mesmos para o disco. Ao fim de algum tempo eles podem eliminar ficheiros, corromper dados ou apresentar simplesmente uma mensagem anomalia. Qualquer que seja o tipo de vírus é sempre importante impedir que entre no sistema.

O vírus pode entrar no sistema a partir da Internet ou por outros meios (em particular através da disquete ou de um CD-ROM). A primeira é através de um ficheiro que tenha sido descarregado de um computador remoto, a outra é no interior de uma mensagem de correio electrónico.

4.8. TROJAN HORSE (CAVALOS DE TRÓIA)

Segundo (Medeiros, 2001) Cavalos de Tróia definem-se como sendo programas projectados para assumir controle de um servidor ou workstation de maneira furtiva, sem que o administrador da rede ou utilizador dê conta.

Para um invasor descobrir quem possui a parte servidora de software faz uma varredura de endereços na Internet. Quem estiver infectado pelo Cavalo de Tróia responderá a varredura.

Os trojans são códigos maliciosos, geralmente camuflados como programas inofensivos que, uma vez instalados no computador da vítima, podem permitir que o criador destes obtenha o controlo completo sobre a máquina infectada. Os programas DoS geralmente são trojans (Medeiros, 2001).

Alguns tipos de Trojans conhecidos, como BO e o Netbus, permitem o acesso ao computador, deixando vulneráveis ficheiros de sistema e senhas gravadas no disco e na memória. Neste caso, um utilizador da Internet infectado por estes pode estar a fornecer sem saber o “passaporte” para a sua senha corrente.

4.9. BACKDOORS

Segundo (Medeiros, 2001) existe uma confusão entre o que é um *Backdoor* e um Cavalo de Tróia, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um Cavalo de Tróia é um programa que cria deliberadamente um backdoor no computador. Programas como browsers, e-mail ou IRC podem possuir backdoors.

Os Backdoors são abertos devido a defeitos de fabricação ou falhas no projecto de programas, isto pode acontecer tanto acidentalmente ou ser introduzido ao programa propositadamente. Por exemplo, programas antigos de IRC possuem defeito que abre um backdoor que permite ao hacker derrubar a conexão do programa com o servidor, fazendo com que ele pare de funcionar.

A maneira mais correcta de se prevenir deste mal é actualizar sempre as versões dos programas instalados no computador, pois nem os programas antivírus são capazes de descobrir os backdoors; Por outro lado os fabricantes de software têm a responsabilidade de avisar aos utilizadores e prover uma nova versão corrigida do programa quando é descoberto um backdoor no mesmo. O uso de firewall também é útil para minimizar este problema, mas não elimina.

4.10. APPLETS

São programas que executam funções mais complexas das páginas da Web; São produzidos pelas linguagens de programação. A *Java* e a *Active X* são usados em complemento do HTML para criar as páginas de Web (Silva et al, 1999).

A pessoa que cria uma página pode, incluir nela quaisquer funções adicionais usando uma destas linguagens (como deslocar um ícone da imagem, criar uma mensagem na base da página, etc.)

A ideia que presidiu ao desenvolvimento destas linguagens é de permitir ao programador criar páginas da Web agradáveis sem que o utilizador se apercebesse de estar a descarregar da rede os pequenos programas necessários para tal. Como pode se entender, estes pequenos programas são uma forma ideal

de criar problemas quando o programador não tem boas intenções. Mesmo o uso de antivírus no computador, não garante protecção contra este mal.

Para contrariar isto, os criadores destas linguagens, a Sun no caso da Java e Microsoft no caso da Active X, tentaram incorporar nelas instrumentos necessários para evitar o seu uso pelos hackers, sendo que os resultados não são garantidos, tendo havido muitos problemas devido à passagem de vírus, em particular, pela Active X. Por outro lado, é impossível configurar o Browser de modo a ignorar estes Applets, se bem que isto se traduza na prática pela impossibilidade de carregar um bom número de páginas na rede (Silva et al, 1999).

4.11. ENGENHARIA SOCIAL

Os administradores de sistemas e analistas de segurança têm a tarefa de garantir que a rede e sistemas estejam disponíveis, operacionais e íntegros, para atingir estes objectivos utilizam ferramentas e tecnologias disponíveis. Não importa quanto dinheiro em equipamentos ou programas forem investidos na segurança, sempre haverá um elemento desprezado: O elemento humano. Muitos atacantes com poucos conhecimentos de programação podem ultrapassar a maioria das defesas utilizando uma técnica designada como Engenharia Social.

Para (Medeiros, 2001) na segurança da informação a Engenharia Social é uma aquisição de alguma informação ou privilégios de acesso inapropriado por alguém do lado de fora, baseado na construção das relações de confiança inapropriadas com as pessoas dentro da organização. Ou seja, é a arte de manipular as pessoas a fazer acções que elas normalmente não fazem.

O objectivo da Engenharia Social, como a técnica de ataque à segurança, é enganar alguma pessoa para que ela directamente forneça informações, ou facilite o acesso a essas informações.

O resultado da acção da engenharia social bem sucedida é o fornecimento de informações ou acesso a intrusos sem nenhuma suspeita do que estão fazendo.

A Engenharia Social é um problema sério. Uma organização deve pregar uma política que possa protegê-la contra esta ameaça, sendo que essa política deve ser repassada para toda a organização. Não adianta implementar as modernas ferramentas de segurança se os funcionários fornecem “a chave da porta” para todos que pedirem (Medeiros, 2001).

CAPÍTULO 6: MÉTODOS E FERRAMENTAS DE SEGURANÇA

Uma vez conhecidas as principais ameaças e técnicas usadas contra a segurança da informação, pode-se descrever as principais medidas e ferramentas de segurança necessárias para eliminar essas ameaças e garantir a protecção do ambiente computacional.

Para contra-atacar as ameaças de segurança descritas no capítulo anterior, a empresa deve estabelecer controles de segurança que serão usadas como base para a criação de um bom modelo de segurança de informações. É nesse sentido que se baseia este capítulo.

1. SEGURANÇA FÍSICA

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas: Incêndios, desabamentos, relâmpagos, cheias, problemas na rede eléctrica, acesso indevido de pessoas aos servidores ou equipamentos da rede, treinamento inadequado de funcionários, etc.

Para as máquinas que pretendem ser fisicamente seguras, deve ser definido que tem acesso ao local. Segundo (Medeiros, 2001), as técnicas de protecção de dados por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida.

2. SEGURANÇA LÓGICA

2.1. AUTENTICAÇÃO

Os serviços de autenticação são um elemento importante em qualquer sistema de segurança na Internet. As entidades que se comunicam na Internet devem ter alguma forma de verificar com quem estão a se comunicar. Essas entidades podem ser pessoas que estejam operando sistemas de computador, ou até dois computadores que estejam se comunicando através de um processo automático.

Nos sistemas computarizados são necessários diversos tipos de autenticação. Diversos métodos e aplicações oferecem serviços de autenticação com diferentes graus de certeza. Em geral quando maior for a certeza necessária para identificar um utilizador na Internet, mais alto será o custo, mais difícil será a utilização do método (Medeiros, 2001).

Segundo (Medeiros, 2001) algumas das formas de autenticação mais usadas no CE são:

2.1.1. Senhas

Senha de acesso é um método mais utilizado, pelas empresas para autenticação dos seus utilizadores. Porém para garantir o seu uso adequado, deve ser definida uma política de senhas, em que sejam criadas regras para a criação, troca e uso das mesmas.

2.1.2. Smart Cards (Cartões Inteligentes)

Na autenticação com Smart Cards é utilizada a combinação de um cartão com uma senha. Smart card é um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais *microchips* embutidos, capaz de armazenar e processar dados.

Um Smart Card pode ser programado para desempenhar inúmeras funções. Pode ser usado tanto para o controlo de acesso lógico como para o controle de acesso físico.

2.1.3. Biometria

Este tipo de tecnologia utiliza a análise de características humanas, como impressões digitais, retina, rosto e de padrões de voz e de assinatura.

A vantagem sobre as outras tecnologias de autenticação é que o utilizador é identificado por características únicas, pessoais e intransferíveis, dispensando o uso de senhas, cartões ou crachás. É também utilizado tanto para controle de acesso físico como para controle de acesso lógico.

2.1.4. On-Time Password

Esta tecnologia consiste em fornecer uma senha de acesso diferente a cada determinado intervalo de tempo (1 minuto, 30 segundos, etc.), permitindo que o utilizador se conecte naquele instante.

As tecnologias de on-time password tornam sem efeito a acção de sniffers, já que a cada conexão uma senha nova deve ser informada, permitindo que seja utilizado um canal seguro.

2.2. SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS)

São sistemas “inteligentes”, capazes de detectar tentativas de invasões em tempo real. Estes sistemas podem apenas alertar sobre a invasão, como, também, aplicar acções necessárias contra o ataque. Eles podem ser Sistemas baseados em regras ou adaptáveis, no primeiro as regras de tipos de invasões e a

acção a ser executada são previamente cadastrados. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre actualizadas para que o sistema seja eficaz. No segundo tipo, são empregues técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem (Medeiros, 2001).

Além disso, o sistema de detecção de intrusão pode ser classificado como NIDS (sistema de detecção de intrusão de redes) e HIDS (sistema de detecção de intrusão de hosts).

2.3. LOGS E AUDITORIA

Do ponto de vista de segurança, auditar é a capacidade de reconstruir um evento relacionado à segurança para auxiliar o exame das causas e efeitos de tal evento. Trilhas de auditoria ou informações de log do sistema podem ser usados para determinar se uma violação da política aconteceu ou se uma actividade suspeita é causa de alarme. Produtos sofisticados para detecção de intrusão, usam trilhas de auditoria do sistema operativo como uma base para sua análise. Elas também fornecem a possibilidade de localizar a fonte de um incidente de segurança complexo e fornecem a evidência necessária para qualquer acção que pode ser requerida.

Segundo (Medeiros, 2001), a capacidade de auditoria de um sistema operativo pode ser avaliada baseando na:

- Amplitude e profundidade de eventos pertinentes à segurança que são suportados;
- Força dos mecanismos disponíveis para proteger os mecanismos de trilhas de auditoria (desligar funções de auditoria ou apagar os logs de auditoria são frequentemente primeira acção que o hacker toma ao penetrar num sistema);
- Suporte para controlar o grande volume de dados de auditoria que um sistema operativo produz.

Os logs desempenham um papel imprescindível no processo de detecção de intrusão. A auditoria e a avaliação destes devem se tornar rotineiras e constantes na vida dos administradores de sistemas a fim de evitar surpresas desagradáveis.

2.4. RECUPERAÇÃO DE DESASTRES E BACKUPS

Pode se definir a recuperação de desastre, como o processo de restauração do sistema após a perda de dados (Medeiros, 2001). Existem diversas ameaças que podem causar desastre no sistema dentre os quais: Força maior, erros inocentes, falhas mecânicas e falhas em programas.

Essas ameaças ou qualquer outra actividade maliciosa influenciam directamente, em vários níveis, na operação de uma empresa. Geralmente quando um desastre ocorre, ao invés de se descobrir a origem, o foco principal é restaurar os recursos de tecnologia da informação para sua total funcionalidade, restaurando as operações de negócio, pois quanto maior for a demora, maiores serão as consequências para a empresa (Medeiros, 2001).

Backups diários ou semanais dos sistemas, incluindo dados essenciais para a operação da empresa, são componentes vitais para a restauração de desastres e para manutenção das funções da empresa.

Para montar um sistema de backups requer-se um pouco de cautela. É importante por exemplo, saber escolher o tipo de dispositivo para armazenar as informações, como fitas magnéticas, discos ópticos mirror, ou sistemas RAID. O dispositivo mais usado é o DAT, pois oferece elevada capacidade de armazenamento, a um custo médio relativamente baixo (Medeiros, 2001).

2.5. CRIPTOGRAFIA

O objectivo fundamental da criptografia é o de esconder a informação criada por uma entidade, de tal forma que apenas outra entidade, autorizada pela primeira, possa aceder ao conteúdo daquela informação. A entidade que cria a informação chamamos *emissor* e quem recebe *receptor*, a informação em si é designada *texto original*, o qual é *cifrado* para esconder o seu conteúdo, obtendo-se deste modo o *texto cifrado*, ou simplesmente a *cifra*. É também comum a utilização de termos como encriptação e encriptar (Silva et al, 1999).

A informação é transformada por um *algoritmo de cifra*, utilizando uma *chave* para transformar os dados, quer se trate de os cifrar ou decifrar. No que respeita a chaves utilizadas, existem duas grandes famílias de algoritmos que serão analisados em seguida.

2.5.1. ALGORITMOS CRIPTOGRÁFICOS

São funções matemáticas usadas para codificar os dados, garantindo sigilo e autenticação. De acordo com a forma de utilização, os algoritmos podem ser divididos em dois tipos principais: Algoritmos de Chave Simétrica e Algoritmos de chave assimétrica (Silva et al, 1999).

2.5.1.1. Algoritmos de chave simétrica ou chave secreta

Neste tipo de algoritmos, a mesma chave é utilizada para cifrar e decifrar os dados (Figura 1), a chave é do conhecimento exclusivo do emissor e receptor. Outro facto determinante é o tamanho da chave, medido em número de *bits*.

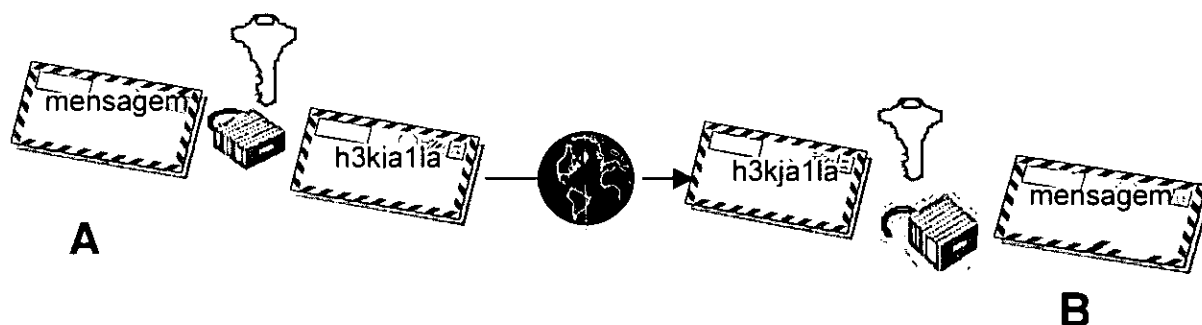


Figura 1. Algoritmo de chave simétrica

A sua implementação é eficiente em termos computacionais e são utilizados para cifrar grandes volumes de dados. No entanto, apresentam uma desvantagem significativa:

O emissor e receptor devem ter conhecimento da chave de forma segura. Se usarem um método inseguro para a distribuir, um adversário pode interceptá-la e decifrar dados cifrados com ela.

Portanto, é necessário recorrer-se a métodos que assegurem a distribuição segura das chaves, em qualquer circunstância. Os algoritmos de chave simétrica mais conhecidos estão descritas nos ANEXOS IV.1.

2.5.1.2. Algoritmos de chave assimétrica ou chave pública

Este tipo de algoritmos usa duas chaves complementares. Dados cifrados com uma chave podem ser decifrados com outra, e vice-versa (Figura 2), neste caso uma das chaves é divulgada publicamente (a *chave pública*), devendo a outra permanecer secreta (a *chave privada*).

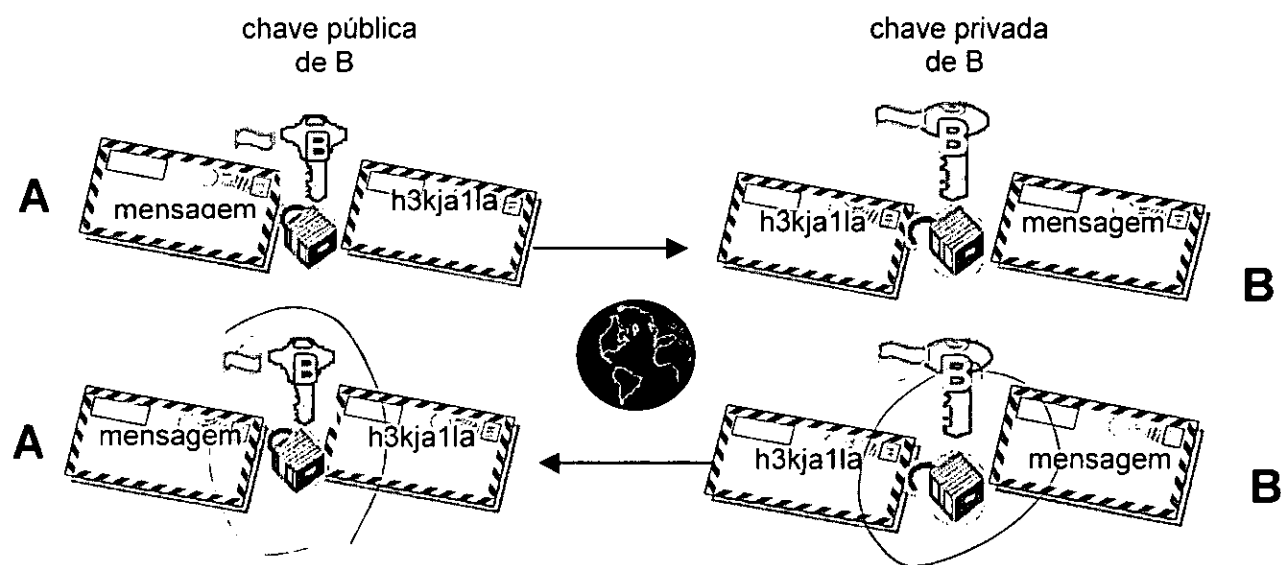


Figura 2. Algoritmos de chave assimétrica

As duas chaves são completamente no sentido de que uma é calculada em função da outra, recorrendo à métodos matemáticos.

O facto de se conhecer a chave pública não fornece qualquer pista para se descobrir a chave privada. A suas desvantagens são:

- A sua implementação é ineficiente devido a complexidade dos métodos nele usado. O que faz com que sejam utilizados para cifrar volumes de dados relativamente pequenos.
- A distribuição das chaves públicas é também um problema, obviamente não ao nível de confidencialidade da chave, mas sim da sua autenticidade.

Os algoritmos da chave pública mais conhecidos estão descritos nos ANEXOS IV.1.

2.5.2. ENVELOPES DIGITAIS

Na descrição dos algoritmos simétricos e assimétricos foram apontadas as grandes vantagens e desvantagens de cada um deles, que podem ser resumidas da seguinte forma:

- Os algoritmos simétricos são eficientes para cifrar grandes volumes de dados, mas a distribuição das chaves é problemática.
- Os algoritmos assimétricos não apresentam grandes problemas na distribuição das chaves (chaves públicas), mas são demasiado complexos para cifrar grandes volumes de dados.

Assim é necessário encontrar um mecanismo que possa aproveitar as vantagens e evitar as desvantagens de cada tipo de algoritmo, para cifrar grandes volumes de dados. Este mecanismo está ilustrado na Figura 3.

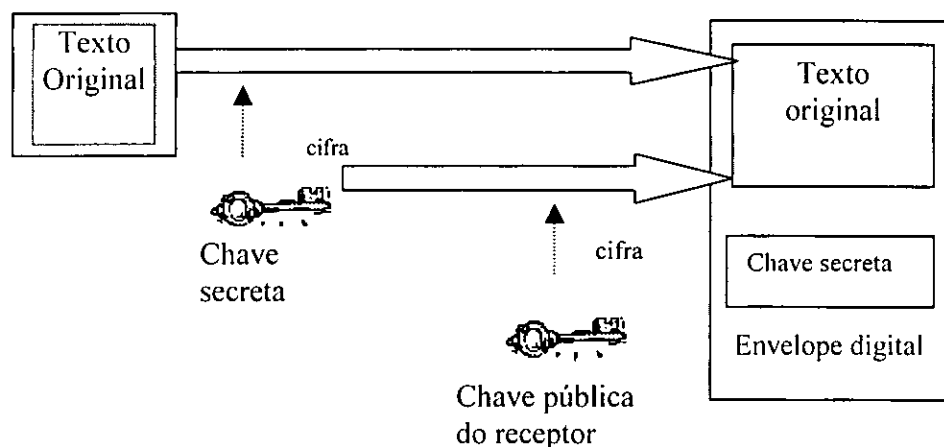


Figura 3. Construção de um envelope digital

Quando o emissor pretende enviar uma mensagem relativamente grande para um receptor do qual conhece a chave pública, começa por gerar uma chave secreta aleatória e usa-a para cifrar a mensagem. Em seguida, cifra esta chave com a chave pública do receptor. Finalmente, envia a mensagem e a chave secreta cifrados ao receptor. O conjunto desses dois elementos é vulgarmente designado por *envelope digital*.

Ao receber o envelope digital, o receptor começa por decifrar a chave secreta com a sua chave privada (como a cifra foi produzida com a chave pública, só a chave privada a pode decifrar). Uma vez na posse desta chave, o receptor pode decifrar a mensagem usando o processo inverso.

2.5.3. ALGORITMOS DE SUMÁRIO

Existem outros algoritmos que não pretendendo esconder a informação, podem ser incluídos na área da criptografia. É o caso do algoritmo de sumário (*hash*), que proporcionam uma forma eficaz de identificar um conjunto de dados através de um valor que os representa unicamente.

Este valor obtém-se através de uma função matemática não inversível, que produz um conjunto de bits de tamanho predefinido (o sumário), a partir de um texto de tamanho arbitrário. Esta função é definida

de forma a ser computacionalmente impraticável determinar qual o texto original a partir do sumário e construir dois textos que tenham o sumário igual (Figura 4).



Figura 4. Algoritmo de sumário

2.5.4. ASSINATURAS DIGITAIS

Já se abordou como os algoritmos simétricos e assimétricos providenciam a confidencialidade da informação e como se pode obter integridade a partir dos algoritmos de sumário. Mas, é também possível usar estes mecanismos para providenciar mecanismos de autenticação e não-repúdio (Silva et al, 1999).

Um emissor que pretenda estas garantias no envio de uma mensagem gera um sumário da mensagem e cifra-o com a chave privada. Em seguida, envia a mensagem, juntamente com o sumário cifrado (Figura 5). Este constitui aquilo que se designa por *assinatura digital*.

Por seu turno, o receptor utiliza a chave pública do emissor para decifrar o sumário. Em seguida, ele próprio gera um sumário da mensagem e compara-o com o que antes decifrou. Se os sumários coincidirem, o receptor conclui que a assinatura digital é válida (Figura 6).

O facto de se conseguir decifrar o sumário com a chave pública do emissor, prova que foi utilizada a chave privada deste, logo apenas este poderia ter cifrado aquele sumário (autenticação).

Por outro lado, o emissor não poderá negar a autoria da mensagem (não-repúdio de criação).

Finalmente, o facto de os sumários coincidirem, prova que a mensagem não foi alterada desde que foi enviada (*integridade*).

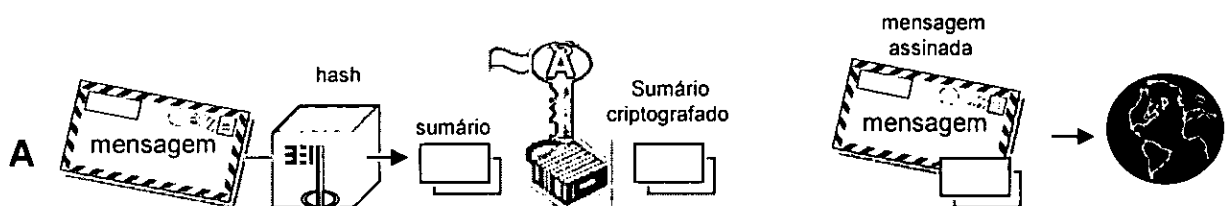


Figura 5. Geração de uma assinatura digital

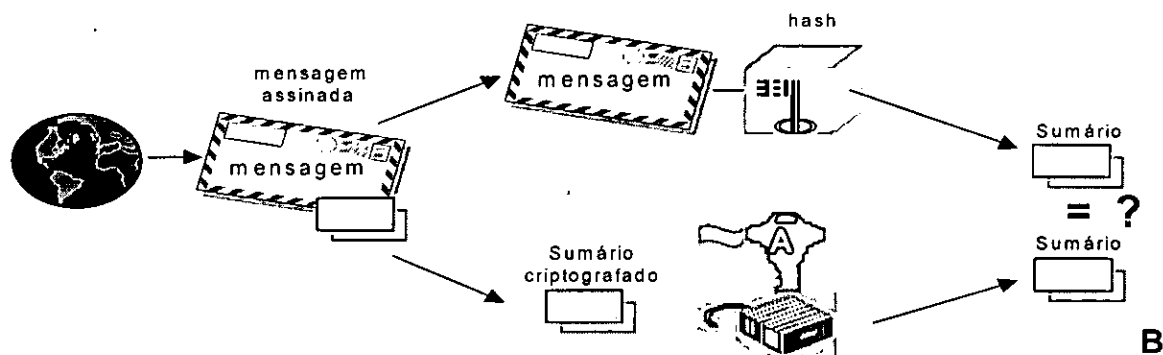


Figura 6. Verificação de uma assinatura digital

2.5.5. CERTIFICADOS DIGITAIS

O certificado digital associa a identidade de um titular a um par de chaves electrónicas (uma pública e outra privada) que, usadas em conjunto, fornecem comprovação da identidade, reconhecida diante de qualquer situação onde seja necessária a comprovação de identidade.

O Certificado Digital é usado no CE. Neste caso, um cliente que compra numa loja virtual, utilizando um “*servidor seguro*”, solicitará o Certificado de Identificação digital deste servidor para verificar: a identidade do vendedor e o conteúdo do certificado por ele apresentado. Da mesma forma o servidor poderá solicitar ao comprador o seu Certificado de Identidade digital, para identificá-lo com segurança e precisão.

Caso qualquer um dos dois apresente um Certificado de Identidade Digital adulterado, ele será avisado do facto, e a comunicação com segurança não será estabelecida.

O Certificado de Identidade Digital é emitido e assinado por uma Autoridade Certificadora (CA). Para tal, esta autoridade usa as mais avançadas técnicas de criptografia disponíveis e de padrões internacionais (norma **ISO X.509 para certificados Digitais**), para emissão e cancelamento digital dos Certificado Digital. Podemos destacar os seguintes elementos do Certificado digital:

- *Informação de atributo*: Informação sobre o objecto certificado. No caso de uma pessoa, inclui o nome, nacionalidade e endereço de e-mail, organização e o departamento onde trabalha.
- *Chave da informação pública*: Chave pública da entidade certificada. O certificado actua para associar a chave pública à informação de atributo, descrita acima. A chave pública pode ser qualquer chave assimétrica, mas usualmente é uma RSA (Silva et al, 1999).

- *Assinatura da autoridade em certificação:* A CA assina os dois primeiros elementos e adiciona credibilidade ao certificado. Quem recebe o certificado verifica a assinatura e acreditará na informação de atributo e chave pública associados se acreditar na CA.

3. MÉTODOS PARA OBTER SEGURANÇA

Falando de métodos a usar para aumentar ainda mais a segurança nas organizações dedicadas ao CE pode-se referir alguns protocolos criados com esse intuito, sendo que cada um deles representa uma aproximação diferente à implementação de comunicações seguras na Internet (Veloso, 2002):

- **SSL** – Secure Sockets Layer
- **PPTP** – Point to Point Tunneling Protocol
- **SET** – Secure Electronic Transaction

3.1. SSL (Secure Socket Layer)

O SSL projectado pela *Netscape Communications Corporation*, a empresa do famoso browser *Netscape*, foi um dos protocolos mais bem aceites pela comunidade da Internet, sendo utilizado por instituições financeiras, negócios de vendas on-line e lojas virtuais, devido à sua fiabilidade e à não interferência por parte do consumidor.

Ao aceder um “site seguro”, o servidor envia para o browser (*Netscape, Internet Explorer, etc.*) o certificado digital nele instalado. O browser verifica a integridade do certificado digital apresentado pelo servidor (utilizando para isso o certificado digital da CA que o emitiu). Esta fase chama-se *handshake*. Não havendo qualquer problema, terá início uma sessão de comunicação segura utilizando-se o protocolo SSL. Uma vez estabelecida a sessão entre dois computadores os dados estão seguros pois são encriptados. O processo é estabelecido entre o consumidor e o fornecedor. Todas as informações relativas à transação electrónica, incluindo o número do cartão de crédito ficam armazenadas no computador do fornecedor.

Apesar da segurança da criptografia na transmissão dos dados, o consumidor não tem a certeza de que o fornecedor está autorizado a receber as informações do cartão de crédito. Mesmo o fornecedor desconhece se o consumidor está autorizado a fazer o débito no cartão.

O maior perigo reside no site do fornecedor. Existe a possibilidade de *oshackers* invadirem e roubar as informações do cartão de crédito para defraudar operações noutros estabelecimentos.

Ultimamente o mecanismo de criptografia do SSL utiliza chave pública RSA com 128 bits para implementar a transmissão segura. Quanto maior o número de bits na chave criptografada, tanto mais difícil será quebrar a chave (Velooso, 2002).

3.2. SET (Secure Electronic Transaction)

Para melhorar o nível de segurança das transações electrónicas foi desenvolvido o protocolo de segurança SET. O SET prevê o envolvimento de 4 componentes: o *Cardholder Wallet* que executa no PC do consumidor, o *Merchant Server* que executa no servidor do fornecedor, o *Payment Gateway* que executa na entidade que liberta os créditos e autoriza a transação e *Certificate Authority* que fornece e autentica as assinaturas digitais do consumidor e fornecedor.

- *Cardholder application*: Também conhecidos por carteira electrónica, é uma aplicação utilizada pelo consumidor que permite o pagamento seguro através da Internet. As aplicações de carteiras electrónicas geram mensagens no protocolo SET que possam ser aceites pelos componentes SET (Merchant, Payment Gateway e Certificate Authority).
- *Merchant Server*: É um produto utilizado pelo comerciante on-line para processar e autorizar os pagamentos por cartão. Ele comunica-se com os componentes Cardholder Application, Payment Gateway e Certificate Authority.
- *Payment Gateway*: É utilizado por organizações que processam as mensagens de autorização e pagamento, emitidas pelo Merchant Server, com as redes das instituições financeiras.
- *Certificate Authority*: Componente usado pelas instituições financeiras ou terceiros previamente aprovados para emitir certificados digitais requeridos por todos os outros componentes.

O SET tem o objectivo de manter as informações críticas guardadas em computadores seguros. Apenas a informação necessária para concretizar uma transação comercial é transmitida. Os dados do cartão de crédito não são transmitidos, apenas existe uma autorização de crédito na conta corrente do fornecedor pela entidade que liberta o crédito, normalmente o banco. Empregando assinaturas digitais, o SET permite a fornecedores verificar se os consumidores são quem afirmam ser. Também protege os consumidores uma vez que providencia um mecanismo de envio dos seus números de cartões de

crédito de maneira a serem transferidos directamente por forma a que a transação seja possível sem que os fornecedores sejam capazes de ver os números dos cartões.

O SET encripta os números dos cartões de crédito que ficam no servidor do fornecedor garantindo assim que só os bancos e as empresas gestoras de cartões de crédito possam lê-los.

O SET utiliza combinações de criptografia DES e RSA. Chaves públicas e privadas são utilizadas por todos os participantes da transação.

3.3. REDES PRIVADAS VIRTUAIS (VPNS)

A área de negócios deseja utilizar a Internet como uma *WAN*, devido aos baixos custos e alcance mundial. A Internet permite minimizar os custos utilizando a sua infra-estrutura para transmitir informação corporativa. Assim surgiu o conceito *VPNs - Virtual Private Networks* (Medeiros, 2001).

Ao invés de depender de linhas dedicadas alugadas ou circuitos virtuais permanentes. Uma VPN baseada na Internet utiliza o *backbone* distribuído e aberto da Internet para transmitir dados entre corporações. Esta rede funciona da seguinte forma: As empresas ligam-se à VPN através de pontos de conexão locais - chamados de pontos de presença, pertencentes ao a *ISP*; A partir daí, é o *ISP* quem garante a transmissão de dados para os destinos apropriados via Internet, ou seja, todos os detalhes da conexão para a rede do *ISP* e a infra-estrutura da Internet são da responsabilidade do *ISP*.

Porém, devido as características da Internet torna-se necessária a inclusão de técnicas de criptografia, para que os dados corporativos transmitidos entre os nós da VPN não sejam interceptados nem corrompidos por terceiros.

3.3.1. PPTP - Point to Point Tunneling Protocol

Os Protocolos de Tunelamento são responsáveis pela abertura e gestão de sessões de túneis em VPNs. O Protocolo de Tunelamento Ponto-a-Ponto (*PPTP*), desenvolvido por um fórum de empresas (*Microsoft, Ascend Communications, 3Com, ECI Telematics e US Robotics*), foi um dos primeiros protocolos de VPN a surgirem. Ele tem sido uma solução muito utilizada em VPNs desde que a Microsoft incluiu suporte para Servidores Windows NT 4.0 e ofereceu um cliente *PPTP* num *service pack* para Windows 95, o que praticamente assegura a sua utilização nos próximos anos (Veloso, 2002).

No entanto, este protocolo apresenta algumas limitações, tais como não providenciar uma forte criptografia para protecção de dados. Para garantir a segurança na transmissão, o PPTP faz uso dos seguintes mecanismos: Controlo de acesso e autenticação, criptografia de dados, filtragem de pacotes PPTP e utilização de *firewalls*.

O PPTP supera a necessidade de uma entidade externa verificar a legitimidade, confiando nas capacidades de segurança do Software. Definir um *userid* e uma *password* para todos os consumidores antes de uma transação não parece exequível, para utilização em à escala Mundial (Veloso, 2002).

4. FIREWALLS

Como o nome sugere, um dos objectivos importantes de um firewall é reduzir danos em caso de desastre, exactamente como acontece quando há um incêndio em um carro ou edifício. No contexto da Internet, os firewalls têm finalidade semelhante - controlar os prejuízos e proteger uma rede, no caso de uma invasão através da Internet. E, um sentido mais genérico, o firewall é usado para regular o fluxo de tráfego entre duas redes (Bernstein et al, 1997).

Segundo (Bortoluzzi, 2001) *Firewalls*, por definição, são componentes ou conjunto de componentes que têm por objectivo restringir acesso entre uma rede protegida e uma pública, que na maioria das vezes é a Internet. O filtro de pacotes é um destes componentes. Tipicamente, a forma mais simples de actuação dos *firewalls* é posicionar um filtro de pacotes no meio da conexão LAN/WAN. Neste caso, o tráfego pode ser restringido interceptando os pacotes com base em um conjunto de regras de comportamento. Por exemplo, a regra *deny tcp from any to 200.169.48.0/24 80* não permite que se acede a porta 80/tcp em nenhum *host* da rede 200.169.48.0. Geralmente, um roteador tem recursos suficientes para implementar este modelo de protecção (Figura 7).

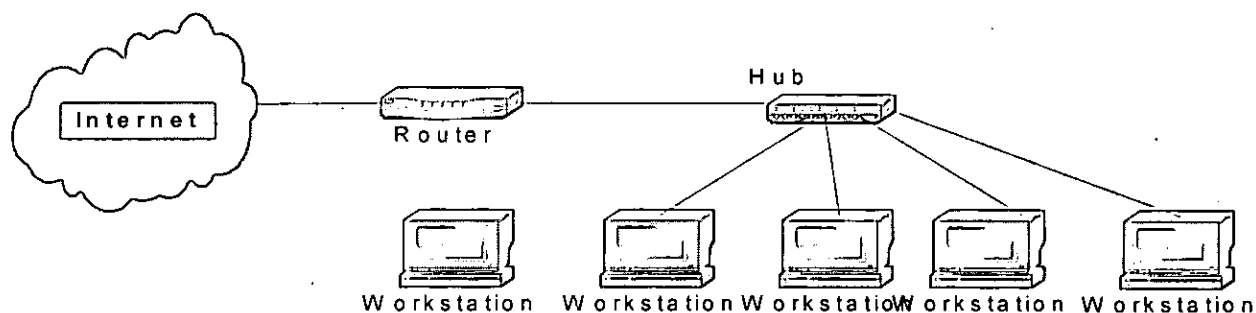


Figura 7. Restrição de acesso implementada no roteador.

Já os *proxy servers* são sistemas que servem como ponto intermediário de entrada e saída para as aplicações da Internet, como o FTP e HTTP. Neste caso, filtra-se o acesso com base em informações mais flexíveis, como o conteúdo das URLs, data e hora, *logins* e outras. Este modelo (Figura 8) geralmente é implementado em um computador com duas interfaces de rede. Uma faz conexão com o roteador, e outra com o concentrador da LAN (*hubs* ou *switches*).

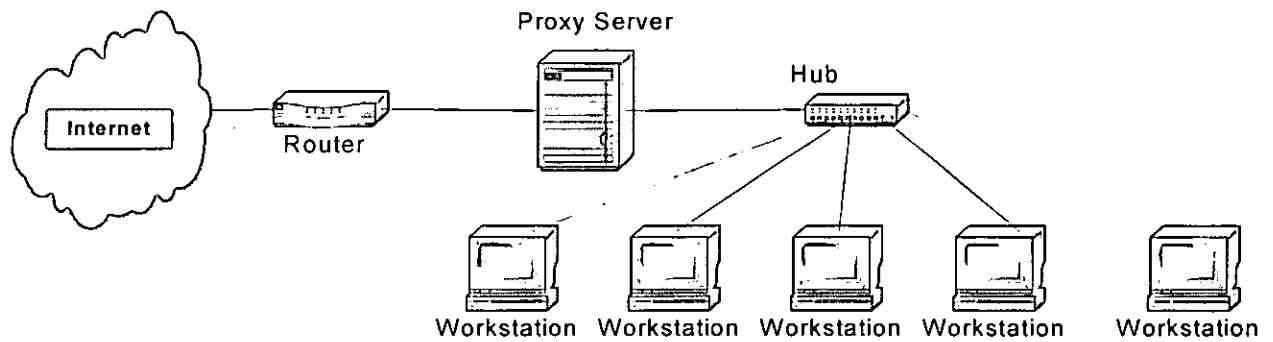


Figura 8. *Proxy server* intermediando conexões

Um *layout* mais aperfeiçoado sugere a presença de um ou mais *bastion hosts* em um perímetro da rede denominado zona desmilitarizada (Figura 9). Neste caso, os computadores da rede interna precisam necessariamente direcionar todas suas solicitações para um dos servidores (*bastion hosts*) que, por sua vez, as redireciona para a Internet. Deste modo, as informações contidas na DMZ ficam protegidas tanto de ataques que tenham origem na Internet como também daqueles que se iniciam dentro da rede local.

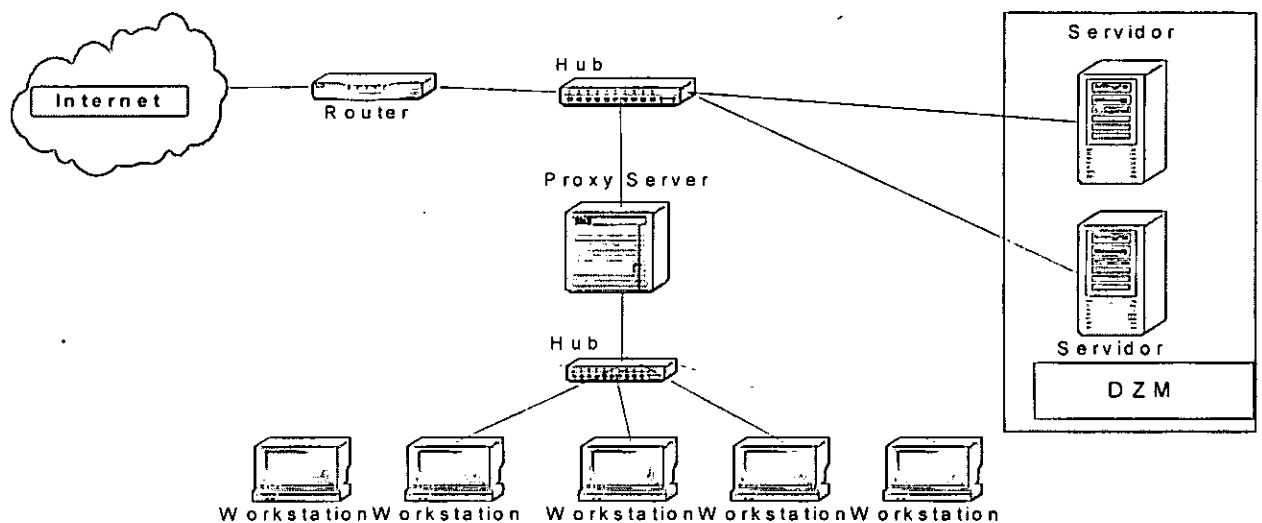


Figura 9. Topologia de acesso a Internet com zona desmilitarizada (DMZ).

4.1. LIMITAÇÕES DE FIREWALLS

Os firewalls não são uma cura definitiva para todos os males de segurança na Internet. Há várias tarefas que os firewalls não são capazes de executar (Bernstein et al, 1997):

- *Os firewalls não garantem a integridade de dados:* Por um lado, os firewalls garantem integridade aos dados da rede interna, protegendo-a do acesso não autorizado, as empresas tentam utilizá-los para detectar vírus. A verificar todo o tráfego recebido não é viável, pois pode provocar a queda de desempenho da rede inspeccionando cada *pacote*.
- *Os firewalls não garantem a autenticidade da origem de dados:* Por natureza, o firewall não têm qualquer controle sobre como o pacote foi criado, ou o que ele faz quando chega ao destinatário.
- *A maioria dos firewalls não garante a confidencialidade de dados:* Por natureza os firewalls não interceptam dados não criptografado.
- *Os firewalls não garantem protecção contra ameaças internas:* A ameaça interna é muito séria e não deve ser ignorada; Para tratar dela, deve implantar firewalls internos.
- *O firewall é apenas um ponto de entrada para uma rede:* Um firewall não oferece protecção contra um tráfego que não passa por ele”.

5. ANTIVÍRUS

Antivírus são programas que detectam, anulam e eliminam os vírus de computador. É preciso monitorar, além do workstation, os servidores, os gateways de e-mail e os firewalls. Com isso, a empresa estará fazendo uma prevenção que pode reduzir drasticamente a ocorrência de invasões (Medeiros, 2001).

A Internet está se transformando no principal meio de contaminação do vírus de macro dentro das empresas. E a fonte de entrada dos vírus são os documentos de texto e folhas de cálculo, ficheiros que são geralmente transferidos para a Web via e-mail.

Actualmente os programas antivírus conseguem eliminar caválos de troia, programas de java e active X hostis e verificam e-mails.

De acordo com (Medeiros, 2001) um bom antivírus deve possuir as seguintes funcionalidades:

- Identificar e eliminar uma boa quantidade de vírus;
- Analisar os ficheiros que estão sendo descarregados pela Internet;
- Verificar continuamente os discos duros e outros dispositivos de armazenamento da informação de forma transparente ao utilizador;
- Criar disquete de verificação que pode ser usado caso o vírus seja inteligente e anule o antivírus que está instalado no computador.

6. NÍVEIS DE SEGURANÇA

6.1. O nível de segurança para o comerciante

Ninguém em on-line está realmente seguro. Mas enquanto Internet apresentar brechas de segurança, a maioria dos vendedores e analistas discute que transações são na verdade menos perigosas no ciberespaço que no mundo físico.

Isso é porque muito das fraudes de cartão de crédito são realizadas no varejo por vendedores que manipulam os números de cartão. Sistemas de CE removem esta tentação codificando os números nos servidores de uma companhia. Para comerciantes, o CE é mais seguro que abrir uma loja que poderia ser roubada, queimada, ou inundada. A dificuldade está em conseguir que os clientes acreditem que o CE é seguro para eles.

6.2. O nível de segurança para o cliente

Consumidores realmente não acreditam nisto, mas os peritos dizem que transações de CE são mais seguras que compras com cartão de crédito no mundo real. Toda vez que alguém paga com um cartão de crédito em uma loja, em um restaurante ou compra por telefone e toda vez que joga fora um recibo de cartão de crédito está vulnerável a fraude.

Os browsers mais populares automaticamente criptografam as informações, quando estão em uma sessão com um site comercial que aceita este tipo de comunicação. A maioria dos sites que lidam com informações sigilosas ou delicadas de seus clientes, como números de cartões de crédito e dados pessoais, utiliza este processo. Chama-se esta comunicação criptografada de "conexão segura", usando

o protocolo SSL. No navegador, pode notar que está no modo seguro quando uma chave aparece no canto esquerdo da janela. O browser exibe um cadeado no lado direito da tela (Figura 10). Outro modo para identificar se um site é assegurado por SSL é quando o URL começa com https: em vez de http.

Nenhum sistema de CE pode garantir 100% de protecção para o cartão de crédito, mas é menos provável ser roubado on-line do que em uma loja real.

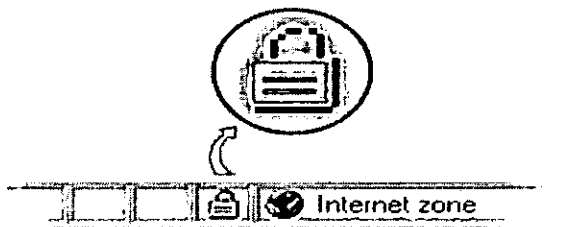


Figura 10. Segurança no navegador

A maior preocupação que se deve ter em relação à segurança das compras através da rede é a confiança depositada no estabelecimento comercial responsável pela venda. Comprando-se em um site respeitado, em que dificilmente ocorrem problemas e decepções.

CAPÍTULO 7: MODELO DE SEGURANÇA PROPOSTO

O enfoque correcto para enfrentar os problemas relativos a segurança no CE se dará através da definição de um plano de segurança (ANEXOS 1.1.) que contemple todas as iniciativas de uma dada organização em relação ao assunto, harmonizando os procedimentos e direccionando os investimentos (Zanini, 2001).

Trata-se de planear as acções necessárias em função das necessidades de segurança levantadas e formalizar tais procedimentos.

Para criação dum modelo de segurança eficaz, em primeiro lugar é necessário que cada empresa faça uma análise de risco para tentar perceber o que pode ocorrer mal isto é, determinar as possíveis ameaças, vulnerabilidades, contramedidas e soluções que garantem um maior nível de segurança para os servidores e a rede da empresa, assim dando suporte ao CE e aumentando a segurança da organização.

1. MODELO PARA PROTECÇÃO DE REDES

O esboço de rede aqui proposto (Figura 11) é inspirado em um protótipo que tem mostrado resultados eficazes segundo (Veen, 2001) e propõe a utilização de apenas um endereço IP válido para toda a rede. Esta situação é muito comum para as empresas que não precisam obter uma classe de endereços ou fracção dela. Em adição, é possível adequar este modelo a redes provedoras de acesso ou redes comerciais, segmentando de acordo com as necessidades.

No presente caso, opta-se por segmentar em três redes distintas: Rede de servidores, rede dos RAS (servidores de acesso remoto) e rede dos workstations. Os RAS são responsáveis por fornecer o serviço de acesso discado aos utilizadores do provedor. O modelo faz uso dos seguintes recursos computacionais:

- Roteador;
- *Bridge Host* (Bridging Firewall) - Filtro de Pacote;
- *NAT Host* (Bastion Host);
- *LOG Host* (Auditoria e Registos);
- As redes de servidores e clientes (DMZ e LAN).

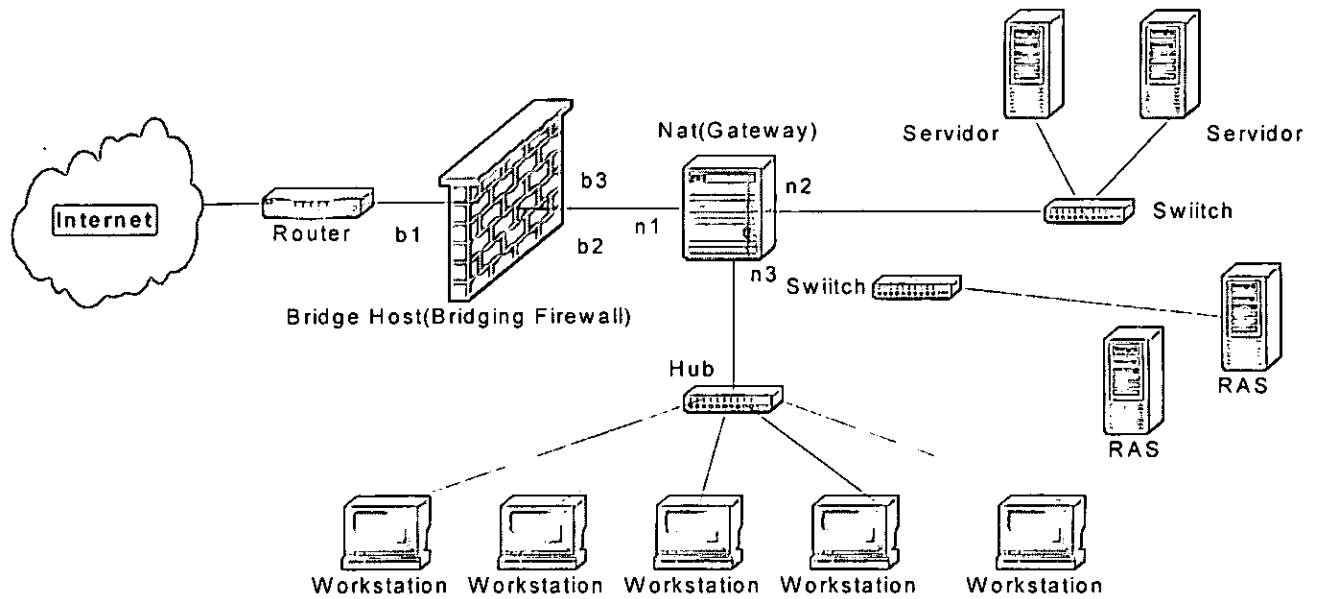


Figura 11. Visão geral do modelo proposto

Ao invés de Hubs utilizados na sub-rede dos workstations, nas sub-redes dos servidores e servidores de acesso opta-se por usar os Switches como forma de garantir maior protecção contra os sniffers. Ao contrário dos Hubs onde todos os pacotes recebidos são encaminhados para todos os workstations conectados a rede local, os Switches direccionam cada pacote recebido por uma das suas portas para uma porta específica de saída, para o encaminhamento ao seu destino final.

1.1. ROTEADOR

Muitos roteadores têm implementado verdadeiros sistemas operativos que possibilitam ao administrador de redes filtrar vários tipos de acesso antes destes entrarem em sua rede. Outros, entretanto, não dispõem de tais ferramentas, restringindo-se somente ao roteamento de pacotes sem analisar em nenhum aspecto o seu conteúdo. Aqui, assume-se que o roteador faça apenas seu trabalho principal, ou seja, o roteamento. A filtragem e o tratamento de pacotes se dará no *Bridge Host*, visto a seguir.

1.2. BRIDGE HOST

Este computador possui 3 interfaces de rede. A primeira (b1) e a segunda (b2) agem como *bridge*. A função principal de um *bridge* é conectar dois segmentos de rede criando a impressão de uma única e grande rede. Neste caso, o *bridge* tem a função especial de filtrar todo o tráfego que passa por ele através de regras que direcionam os pacotes, bloqueando os indesejados.

O que se vê hoje é o computador que age como *proxy* fazendo este trabalho. A desvantagem nisso é que o *firewall* é visível (acessível) na Internet. No caso aqui proposto as interfaces (b1) e (b2) *não recebem endereçamento IP*. Este procedimento assegura que nenhum computador - tanto na rede interna como na externa - saberá de sua existência. Portanto ele não pode ser acedido via Internet nem ser atacado no nível do protocolo IP.

A terceira interface (b3) existe para uma finalidade muito importante: Ela é a responsável por enviar logs ao *LOG Host* sobre as actividades suspeitas e as tentativas de invasão para que sejam reportadas, bem como receber novas regras de filtragem de emergência sobre acessos indevidos detectados pelo IDS que estão em cada segmento de rede. Esta interface necessita de um endereço IP, porém o trabalho de *bridging* entre (b1) e (b2) ocorre de tal forma que elas são incapazes de trocar informações com (b3).

1.3. NAT

A tecnologia NAT (*Network Address Translator*) permite que computadores configurados com endereços não roteáveis possam enviar e receber pacotes pela Internet. Os motivos para o uso deste recurso são estes:

- Escassez de endereços válidos: Muitas vezes o custo para se alocar um endereço válido para cada computador em uma rede pode inviabilizar o acesso a Internet.
- Segurança: Já que nas organizações a maioria dos computadores faz uso da Internet para aceder recursos e não para servir conteúdo é mais seguro fornecer a estes computadores um endereço que não pode receber pedidos de conexão originados de fora da rede local.

O Modelo então requer um computador que seja capaz de assumir pedidos originados na rede interna, processá-los e devolver os resultados ao computador que fez a solicitação.

Este *host* necessita de 3 interfaces de rede. A primeira (n1) entrega todo conteúdo que recebe de (n2) e (n3) para a interface (b2) presente no *Bridge Host*. A segunda (n2) é o *gateway* para todos os servidores da corporação. A terceira (n3), por fim, é o *gateway* de todos computadores que não servem conteúdo, ou seja, os workstations.

A separação entre rede de servidores de workstations fornece o benefício de que se uma vulnerabilidade for encontrada e explorada por um *hacker* nos serviços (DNS, SMTP, HTTP...) de um dos servidores, os computadores da rede de workstations ainda estarão protegidos de tal ataque.

O *bastion host* é o primeiro computador (se não o único) com presença real na Internet. Desta forma, ele é o sistema exposto a elementos muito hostis. É nele que todos utilizadores - inclusive os que agem de má fé - devem se conectar para aceder todos os outros sistemas e serviços.

O *bastion host* está altamente exposto porque a sua existência é conhecida na Internet. Portanto, o responsável pela manutenção do sistema deve concentrar esforços de segurança nele. Mesmo falando-se em um único *bastion host*, é importante saber que pode haver mais de um, dependendo da configuração do *firewall*. O número depende dos requerimentos de cada *site* em particular, mas o princípio é sempre o mesmo.

Bastion hosts são usados de várias formas em várias topologias. A maioria, entretanto, é orientada à filtragem de pacotes, ao *proxying* (*procuração*) ou a ambas. Em uma abordagem híbrida seus princípios gerais devem ser:

- *Orientação à simplicidade*: Quanto mais simples for um *bastion host*, mais facilmente pode-se manter seguro. Qualquer serviço que o *bastion host* ofereça pode conter *bugs* de *software* ou erros de configuração que acarretam problemas de segurança. Portanto, deve-se ter em mente a importância em manter a simplicidade e oferecer o menor número de serviços possível neste sistema - e com os mais baixos privilégios - mantendo assim, a rede sem criar nela um gargalo.
- *Preparação para o comprometimento do sistema*: Por mais que se empreenda todos os esforços para garantir a segurança do *bastion host*, pontos de quebra(ou, pontos de entrada) podem ocorrer. Subestimar o quão seguro é este sistema deve ser regra para o administrador de sistemas. Somente preparando-se para o pior, e planejando - se para que seja possível reverter este facto.

Caso o *bastion host* venha a ser comprometido, deve-se evitar que esta quebra leve a um desastre do sistema de protecção por completo, instruindo os servidores de conteúdo a não aceitar nenhuma conexão com origem no *bastion host* excepto aquela que justifica a existência do servidor em questão. Por exemplo: negar, no filtro do servidor HTTP qualquer conexão originada no *bastion host* com destino diferente da porta 80/tcp.

1.4. O LOG HOST

Mesmo que o servidor que dá acesso ao CE fosse devidamente protegido, ataques podem ocorrer por isso, é necessário implementar o *Log Host* que trata-se de um computador, isolado fisicamente dos demais e, preferencialmente, conectado através de uma comunicação serial ou qualquer outra inalcançável por qualquer intruso. Seu papel é receber e registrar eventos que estão ocorrendo na rede, bem como colectar provas que eventualmente possam incriminar o intruso que atacar o perímetro monitorado.

Este servidor utilizará um programa chamado **SyslogNG**, que é compatível com o padrão Syslog do Unix e permite uma maior filtragem de informações.

Todos os servidores, e equipamentos que possuem o serviço de log, devem ser configurados para enviar mensagens ao servidor de logs ao invés de mantê-las localmente. Por sua vez o Log Host filtra essas mensagens e as armazena de acordo com a sua classificação, facilitando o trabalho de auditoria.

1.5. AS REDES DE SERVIDORES E WORKSTATIONS

Estando protegida tanto por um filtro de pacotes invisível quanto por um *gateway* desempenhando tradução de endereços, as redes de servidores e workstations estão relativamente protegidas. As medidas tomadas neste modelo elevam ao máximo o nível de segurança entre os computadores que formam estas redes. Porém, isto não significa que a barreira seja intransponível. Por mais que se inspecione todos os pacotes, quando o serviço parecer legítimo ele deve ser atendido. Deste ponto em diante, é possível ao atacante agir de duas formas:

- *Causar negação de serviço*: Sendo os pacotes legítimos, eles devem ser atendidos. Porém, se o *hacker* fizer muitos pedidos de conexão antes de receber confirmação, configura-se um ataque de negação de serviço.

Geralmente um computador só, não consegue causar tal efeito, mas uma rede distribuída de atacantes consegue este intento, principalmente escolhendo como alvos grandes empresas comerciais.

Não existe solução que garanta com sucesso a protecção de uma rede contra estes ataques. O que se pode fazer é utilizar um sistema de detecção de intrusos activo que monitora o sistema e se encontrar alguma actividade suspeita, instrui o filtro de pacotes a não mais aceitar qualquer conexão com o endereço de origem do atacante. Neste caso, para evitar a sobrecarga de informação (*flood*) deve-se enviar uma única notificação ao administrador sobre o ocorrido e rejeitar os demais pacotes, evitando assim, entupir o *Log Host* com mensagens repetidas.

- *Explorar falhas de implementação dos softwares que realizam serviços:* Quando todos os componentes de segurança estão activos e no máximo de sua performance, incluindo o sistema que controla e evita ataques de negação de serviço ainda pode haver falhas nos *softwares* que servem os computadores da rede.

Estas falhas são brechas deixadas pelos programadores da implementação de um serviço descobertas por *hackers* experientes.

1.6. REQUISITOS PARA A IMPLEMENTAÇÃO DO MODELO

1.6.1. HARDWARE

A montagem do bridge requer os seguintes componentes de Hardware:

- Microprocessador Intel Pentium 100 Mhz com 32 Mb de RAM e disco duro de 1Gb;
- Duas interfaces de rede ethernet 100 BASE TX;
- Um cabo cross-over (EIA/TIA 586-A/568-B).

1.6.2. SOFTWARE

Em termos de software, são necessários:

- Sistema operativo **FreeBSD, versão 4.5-RELEASE** ou mais recente;
- Detector de intrusos **Snort Versão 1.8.4** ou mais recente;
- Script para bloqueio de acesso **Guardion 1.7** ou mais recente.

1.6.2.1. O SISTEMA OPERATIVO DO BRIDGE HOST

O **FreeBSD** é um sistema operativo BSD UNIX profissional, para computadores com processadores baseados no modelo i386, DECAAlpha ou PC-98.

Derivado do último *release* do BSD UNIX (versão 4.4), o FreeBSD herda a implementação do protocolo TCP/IP que deu origem a ArpaNet e posteriormente a Internet.

Entre os motivos para esta escolha, estão:

- Possui filtro-de-pacotes (*firewall*) incorporado ao *kernel* do sistema;
- O acesso a seu código fonte, além de ser didáctico, permite ajustes de performance e segurança;
- Tem como princípios a estabilidade, segurança e uniformidade de uso;
- Possui, historicamente, a melhor implementação do protocolo TCP/IP entre todos sistemas operativos;
- Não há custos financeiros com licenciamento;
- Possui um dos históricos de menor número de falhas que possibilitam acesso indevido ao sistema.

Como a maioria dos sistemas UNIX, o FreeBSD permite:

- partilha de ficheiros via NFS;
- Distribuição de informações de rede via NIS;
- *Logins* remotos via SSH;
- Monitoramento remoto, incluindo carga do processador, memória, interfaces de rede, estado de processos via SNMP;
- Código para configuração de *bridge* mais estável do que os outros sistemas operativos.

A instalação do FreeBSD é feita com base nas instruções especificadas nos ANEXOS III.1.

1.6.2.2. DETECTOR DE INTRUSOS

O **Snort** (Snort, 2002) é um sistema detector de intrusos em rede. Entre outras capacidades, ele pode ler um conjunto de regras e compará-las com o tráfego da rede. Quando o padrão é reconhecido, o programa regista a actividade suspeita e emite uma alerta ao administrador. A sua instalação é feita com base nas instruções especificadas nos ANEXOS III.2.

1.6.2.3. BLOQUEADOR DE ACESSO

O **Guardian** (Guardian, 20002) é um programa que actualiza automaticamente o filtro de pacotes com base nas alertas geradas pelo Snort. Desta forma, o firewall bloqueia todos os endereços IP com origem no sistema ou rede do atacante. Os passos da sua instalação estão descritos nos ANEXOS III.3.

1.7. VPNS ENTRE OS SERVIDORES

Os equipamentos dentro de servidores precisam comunicar-se para troca de informações sobre autenticação de utilizadores, consultas na base de dados e para envio de mensagens ao servidor de logs. A maioria dessa comunicação trafega sem criptografia, dessa forma se um invasor comprometer alguma máquina do segmento ele poderá monitorar o tráfego. Mesmo que este segmento esteja a usar um Switch para maior protecção com os Sniffers, existem formas de ataque que fazem com que o Switch se comporte como um Hub.

Para proteger os dados e garantir a confiabilidade pode se implementar VPNs entre servidores que necessitam de se comunicar. Pode ser utilizado o programa **VTUN**, que usa o algoritmo *Blowfish* que é leve ao mesmo tempo sem perder segurança. A configuração do VPN é muito simples, depois de estar a funcionar ele cria interfaces de rede virtuais nas quais todos os dados trafegados são criptografados.

A utilização de VPNs não tem grandes reflexos na performance da rede, não afecta a execução de nenhum serviço, mas sim torna a comunicação entre os servidores mais segura.

2. SEGURANÇA NO SERVIDOR DO COMÉRCIO ELECTRÓNICO

Para a execução do sistema de CE propõe-se a utilização de um servidor independente, pois quando este compartilha outros serviços utilizados pelos utilizadores, torna-se mais difícil garantir a sua segurança. Além disso quanto maior o número de serviços em um servidor, maior é a probabilidade de ser descoberta uma falha de segurança em seus sistemas. Sendo assim é necessário instalar e configurar um servidor do CE que fornece apenas serviços de servidor Web com criptografia SSL e servidor de base de dados. Este servidor deve utilizar um sistema **RAID 1** que faz o espelhamento de discos para garantir a disponibilidade da informação no caso de uma falha física em algum dos seus disco.

2.1. PROTEÇÃO DE DADOS NO SERVIDOR

Para a protecção da confiabilidade e integridade de dados trafegados através da conexão entre os clientes, lojas virtuais e o sistema, usar-se-á o protocolo **SSLv2** através do programa **ModSSL**. Este programa actua como um módulo que é agregado ao servidor Web da organização.

Para o correcto funcionamento do SSL é utilizado o certificado digital fornecido por alguma autoridade certificadora reconhecida, esse certificado garantirá a identidade do servidor aos clientes. Sem o certificado, a comunicação SSL pode até ser estabelecida, mas o browser Web do cliente vai emitir uma alerta informando que a identidade desse servidor não pode ser verificada.

Neste caso o SSL usado contém um certificado de 128 bits, o que pode garantir a segurança de dados trafegados na Internet, assim protegendo informações importantes como o número do cartão de crédito e dados particulares dos clientes.

Para assegurar que os dados enviados pelo sistema do CE aos administradores de lojas virtuais, não se armazena nenhum dado importante como o número de cartão de crédito no servidor da base de dados do CE. Assim que os pedidos de compra são efectuados esses dados são criptografados, através do software **GRUPC**, e enviados directamente para os lojistas onde a transação é finalizada. Para assegurar esse novo envio usa-se uma chave assimétrica de 4096 bits.

Para cada loja virtual implantada é criado um par de chaves que é instalado no computador localizado no estabelecimento físico do cliente, responsável por receber pedidos provenientes do sistema de CE. No servidor ficam localizadas as chaves públicas das lojas virtuais, quando o pedido é efectuado, os dados são criptografados e enviados aos lojistas.

O processo tornar-se-ia mais seguro com a utilização do protocolo SET, pois neste caso nem mesmo os lojistas teriam acesso aos números de cartão de crédito dos clientes, esses dados seriam directamente enviados para a operadora de cartão de crédito que autorizaria a compra e a transferência de fundos electronicamente para a loja, mas a utilização do SET envolve mais custos para lojas virtuais, tornando mais difícil a aceitação desta tecnologia.

Mesmo com a utilização do protocolo SSL, com as tecnologias aqui propostas é possível garantir um elevado nível de segurança, onde somente os lojistas tem acesso aos dados dos seus clientes.

Caso o servidor viesse a ser comprometido, nenhum dado importante sobre clientes estaria disponível na base de dados, diminuindo consideravelmente as consequências de um ataque.

2.2. ARMAZENAMENTO DE BACKUPS

Para a protecção de backups pode ser aplicada a criptografia com chave assimétricas utilizando o programa GNUPG. Pode-se criar duas chaves de 4096 bits, um par contendo chave pública e privada de servidores, e outro par contendo as chaves do grupo de administradores de sistemas. Sempre que as cópias são geradas nos servidores, elas serão automaticamente criptografadas utilizando chave pública da equipa de administração de sistemas, as cópias devem ser assinadas digitalmente com chave privada dos servidores. Assim somente os administradores, na posse da chave privada podem decifrar os dados armazenados nos backups e ainda confirmar a sua origem e integridade através da comparação da assinatura digital com a chave pública dos servidores.

Com esta protecção, mesmo que a cópia levada por um dos sócios da empresa seja roubada, as informações contidas nela estariam seguras. Além disso, somente os funcionários autorizados tem acesso aos dados de backups, pois apenas eles tem acesso a chave privada necessária para aceder os dados.

3. AUTENTICAÇÃO

Para a escolha das senhas os utilizadores devem usar um programa que têm função de gerar aleatoriamente as senhas(Random Password Generator), este tipo de programa pode ser encontrado facilmente na Internet. Através dele é possível criar senhas difíceis de quebrar, uma vez que ele gera uma combinação de caracteres sem nenhum significado.

Além de utilizar senhas seguras, é importante troca-las com frequência, pois alguém já pode ter descoberto uma senha, ou pode estar tentando descobrir. *Por outro lado é necessário preparar os sistemas para expiração automática das senhas num período de dois meses.*

4. PROTECÇÃO CONTRA VÍRUS E CAVALOS DE TRÓIA

A protecção contra vírus e outras pragas virtuais é um ponto muito importante na segurança da organização.

Para a protecção de servidores e workstations pode se instalar o antivírus **AVP**. Este programa fica residente em memória a procura pela execução de qualquer código malicioso conhecido, ainda é possível fazer verificação manual nos ficheiros do sistema. O programa ainda permite a actualização automática através da Internet.

5. SEGURANÇA FÍSICA

Para solucionar este problema deve se definir regras de quais pessoas tem acesso aos servidores, inicialmente somente os administradores de sistemas tem acesso para tal. Além disso, para garantir a segurança física dos equipamentos, pode se instalar um ponto de alarme nesse local.

Para garantir a disponibilidade é necessário revisar todas as instalações eléctricas, assim como instalar ar condicionado para manter a temperatura da sala.

6. ATAQUES INTERNOS E ENGENHARIA SOCIAL

Este ponto não pode ser desprezado, pois a Engenharia Social pode ser utilizada para obter informações. Dessa forma deve-se educar os funcionários no qual foram determinadas as suas responsabilidades para a manutenção da segurança da informação, além de definir quais informações são sigilosas e de propriedade da empresa.

No âmbito técnico, a utilização de um firewall para o controle de tráfego, o SSH para gestão dos servidores e os sistemas de IDS possibilitam um maior controlo de acessos internos e identificação de possíveis ataques.

7. GESTÃO DE SERVIDORES

A equipa de administração de sistemas necessita constantemente de aceder remotamente os servidores para manutenção e implementação de novas tecnologias. Para possibilitar essa tarefa pode se usar o protocolo SSH através do programas **OpenSSH**. Este programa torna possível o acesso remoto ao *shell* dos servidores de forma segura, ele criptografa todo o tráfego da transmissão, impedindo que possam ser capturados comandos ou senhas. Este programa ainda permite a autenticação dos utilizadores através de chaves assimétricas. Sendo assim para a autenticação cria-se um par de chaves para cada um dos administradores de sistemas, as chaves públicas destes são instaladas nos servidores e as privadas

em suas workstations. Desta forma, o acesso é permitido aos administradores na posse da sua chave privada.

O uso da criptografia assimétrica para autenticação permite uma segurança incomparável com a utilização de senhas, pois ela elimina a possibilidade da quebra deste controle.

8. RESPOSTA A INCIDENTES

Deve se criar um plano de resposta aos incidentes, nesse documento devem constar informações sigilosas sobre pessoas responsáveis e os procedimentos que devem ser adoptados no caso de incidentes envolvendo a segurança das informações. Os principais pontos a serem colocados no plano de resposta à incidentes são:

- Procedimentos para identificação e auditoria de problemas;
- Divulgação de informações;
- Procedimentos e pessoal responsável pela restauração dos sistemas;
- Contactos com as fontes do ataque e com os órgãos de segurança;
- Procedimentos para isolamento de sistemas.

CAPÍTULO 8: AVALIAÇÃO DO MODELO

Uma proposta de modelo precisa ser avaliada tomando como base o impacto que poderá trazer após a sua implantação, ou seja, submeter a uma avaliação em discussões e reuniões em que participam os gestores e especialistas no domínio do problema.

A avaliação do modelo proposto foi feita com os seguintes objectivos:

- Certificação da obtenção dos objectivos esperados a partir de medições e percepções das pessoas;
- A possibilidade de implementação do modelo tendo como base os mercados nacional ou mesmo internacional;
- Grau de aceitação modelo pelos administradores de sistemas e redes.

De acordo as discussões e reuniões efectuadas com os administradores de redes e sistemas de algumas empresas nacionais, a avaliação feita é que o modelo proposto satisfaz em grande parte as necessidades das instituições que se dedicam as actividades comerciais, ou seja que usam o comércio electrónico como fonte de rendimento, pois introduz conceitos de segurança tanto ao nível da rede, dos equipamentos assim como dos dados que trafegam em tais redes e que estão armazenados em equipamentos electrónicos. Isto é feito usando ferramentas cuja a aquisição é de custo relativamente baixo tanto em termos de Software e Hardware.

As ferramentas de software proposta são modernas e permitirem um fácil ajuste em termos de performance e segurança, para além de possuírem um menor número de falhas o que incapacita a acção dos invasores.

O outro facto determinante é interoperabilidade do modelo, isto é, a especificação é aplicável em uma variedade de plataformas de hardware e software, sem incluir uma preferência de uma sobre a outra. Por exemplo, qualquer portador de um cartão de crédito com software compatível está habilitado a se comunicar com o software do comerciante que também faz parte do padrão definido.

Por outro lado estas ferramentas permitem um administração remota de todos os recursos, ao invés de dispor estas ferramentas em diversas máquinas espalhadas pela rede.

CAPÍTULO 9: CONCLUSÕES E RECOMENDAÇÕES

É seguro afirmar que a informática contribui com mudanças significativas nos sectores de comércio e serviços. A Internet mudou a política de fazer comércio e promete também inovações na área de serviços, que não é tão difundida actualmente.

O CE via Internet permite que empresas de pequeno porte possam competir com grandes empresas, além de estreitar laços entre clientes e fornecedores, ampliando a abrangência da empresa.

O principal ponto que limita o crescimento e aceitação ampla do CE é a suposta falta de segurança. A segurança ainda não pode ser garantida, mas os riscos que ocorrem no ambiente virtual quando da compra de algum bem são os mesmos que podem ocorrer no mundo real.

Perante o que foi referido até agora não subsistem dúvidas de que é essencial ter uma política de segurança e efectuar controlo de acessos. Existem soluções mais económicas e mais dispendiosas. A direcção a seguir terá de ser orientada pelas necessidades de segurança que a organização tem.

O conhecimento e a utilização das ferramentas de auxílio na detecção e bloqueio de intrusões está se tornando um dos factores crítico de sucesso no cumprimento da política de segurança pois fornece recursos para investigar os pacotes de dados antes que estes atinjam os servidores da corporação evitando na maiorias das vezes ataques comprometedores.

A infra-estrutura, procedimentos e recursos de segurança devem ser vistos com prioridade e estar em constante reavaliação dentro das corporações. Como em consequência do cenário ao mesmo tempo amigável e hostil que a Internet oferece.

O objectivo de reavaliar segurança nas organizações, imposta pela nova realidade global, não deve tirar o foco de negócios. Por outro lado, não é desejável que se tome decisões a partir de análises superficiais ou de direccionamentos extremistas e pouco flexíveis, fundamentados simplesmente por medo e insegurança.

Acredita-se que o modelo apresentado neste trabalho é de grande utilidade para as organizações que se dedicam ao CE, sendo que os objectivos previamente especificados neste trabalho foram alcançados, apesar de ter-se verificado vários constrangimentos no decurso do trabalho em relação a busca de informação, dado que a matéria abordada ainda trata-se duma novidade no nosso país.

RECOMENDAÇÕES

- Implementação de Cluster para o servidor de Comércio Eletrónico, a fim de garantir maior disponibilidade;
- Testar o uso de outros sistemas operativos para além de FreeBSD e OpenBSD, e suas ferramentas de segurança;
- Realização de testes de penetração para comprovar a validade das medidas e ferramentas de segurança aplicadas no modelo;
- Manter actualizado o sistema detector de intrusos em rede(Snort);
- Disseminar a cultura de segurança tanto para membros da corporação, parceiros de negócios e clientes;
- Implementação deste modelo, para a simulação da eficiência do seu funcionamento;
- Divulgação do modelo.

CAPÍTULO 10: BIBLIOGRAFIA

I. REFERÊNCIAS BIBLIOGRÁFICAS

- (Silva et al, 1999) Silva, M. M.; Silva, A. R.; Nuno, A. R.; Conde, A. (1999), Comércio Electrónico na Internet. Lisboa, FCA.
- (Bernstein et al, 1997) Bernstein T.; Bhimani, A.B.; Schultz, E.; Siegel, C. A. (1997), Segurança na Internet. Rio de Janeiro, Editora Campus.
- (Ferrão, 2000) Ferrão F. (2000), E- Business. Lisboa, Escolar Editora.
- (Veen, 2001) Veen, J. S. V. D. (2001), A Network Setup with FreeBSD and OpenBSD. <http://www.daemonnews.org/200109/contents.html>. 15-08-2002.
- (Medeiros, 2001) Medeiros, C.D.R (2001), Segurança de Informação. <http://www.expresso.com.br/carlos/tce.html>. 09-06-2002.
- (Bortoluzzi, 2001) Bortoluzzi, F. (2001), Estratégias de Segurança. <http://www.modulo.com.br/pdf/ta0111fbortoluzzi.pdf>. 01-08-2002.
- (Zanini, 2001) Zanini, A.S. (2001), Proposta de implementação de uma política de controle de acesso as informações em ambiente de microinformática. <http://www.scua.net>. 09-05-2002.
- (Snort, 2002) The open Source Network IDS. http://www.snort.org/docs/writing_rules/. 07-07-2002.
- (Velooso, 2002) Velooso, C.J.M.(2002), Criptografia -Uma ciência fundamental para tratamento de informações sigilosas. <http://www.modulo.com.br>. 09/06/2002:
- (Guardian, 2002) Guardian Active Response for Snort. http://www.freebsd.org/doc/en_US.IS08859-1/books/handbook/install.html. 07/07/2002
- (Albertini, 2000) Albertini, A. L. (2000). Comércio Electrónico. 2ª Edição. São Paulo, Atlas.

2. BIBLIOGRAFIA CONSULTADA

- Cisneiros, H. (1998), Segurança em Linux. <http://www.netdados.com.br/newsgen/tml/tm13.4/g06.html>. 03-05-2002.
- Simon C. (1998), Negociar na Internet. Lisboa, Editora Presença.
- Jacomo, D. B. P. (2000), Segurança em Windows NT 4.0. http://www.rnp.br/newsgen/001/seg_nt4.shtml. 27-05-2002.
- Gomes, O. J. A. (2000), Segurança Total – Protegendo-se contra os Hackers. São Paulo, Makron Books.
- Roesch, M. (2002), Snort Users Manual. http://www.snort.org/docs/writing_rules. 15-08-2002.
- Sousa, I. D. (1997), Negócios & Internet. Lisboa, FCA.
- Fantinatt, J. M. (1988). Segurança em Informática – Metodologia e Prática. São Paulo., McGraw - Hill.

ANEXOS

ANEXOS I

ANEXOS I.1. PLANO DE SEGURANÇA DE INFORMAÇÃO

ANEXOS II

ANEXOS II.1. TABELA DE FERRAMENTAS PROPOSTAS

ANEXOS III

ANEXOS III.1. CONFIGURAÇÃO DO SISTEMA OPERATIVO FREEBSD

ANEXOS III.2. INSTALAÇÃO DO DETECTOR DE INTRUSOS (SNORT)

ANEXOS III.3. INSTALAÇÃO DO GUARDIAN

ANEXOS IV

ANEXOS IV.1. ALGORITMOS DE CHAVES SIMÉTRICAS

ANEXOS IV.2. ALGORITMOS DE CHAVES ASSIMÉTRICAS

ANEXOS V

ANEXOS V.1. PROTOCOLO TCP/IP

ANEXOS VI

ANEXOS VI.1. QUESTIONÁRIO

ANEXOS I

ANEXOS I. PLANO DE SEGURANÇA DE INFORMAÇÃO

Segundo (Zanini, 2001), a Figura I. Mostra o resumo de acções necessárias para dotar qualquer organização de segurança de informações. Este é um modelo com fases clássicas cujos os resultados de cada uma subsidiam as fases posteriores, formando assim uma cadeia de acções.

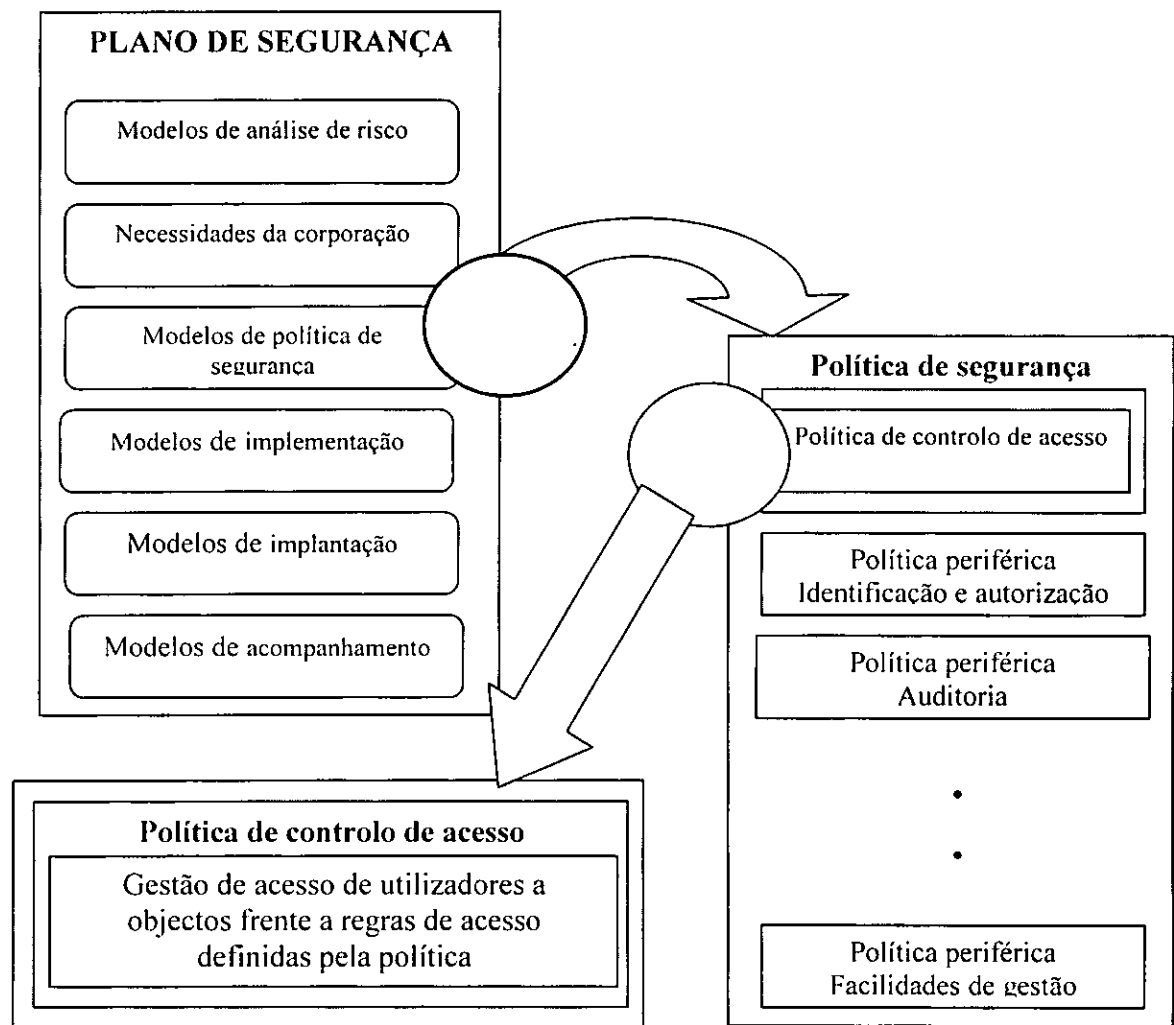


Figura I. Blocos que compõem a política de segurança

Um plano de segurança voltado a informática deve ser tratado de uma forma global para prover segurança a um sistema computarizado utilizado por um grupo de pessoas ou corporação.

Para dar forma a elaboração e a aplicação do mesmo, é recomendada a divisão em um conjunto de fases, cada qual objectivando subsidiar a fase posterior. Trata-se de um série de acções a serem desenvolvidas de forma a prover segurança voltada ás necessidades das instituições.

Para que haja o desenvolvimento e implementação de um plano de segurança de informações, certamente, deverá optar-se por uma política favorável á cultura organizacional, enfocando os pontos de riscos e fixando objectivos a serem alcançados em função dos recursos disponíveis.

As fases para confecção de um plano de segurança voltadas para as corporações, podem ser escritas segundo um modelo apresentado por Sandu, Coyne, Feinstein e Youman, conforme ilustra a Figura II.

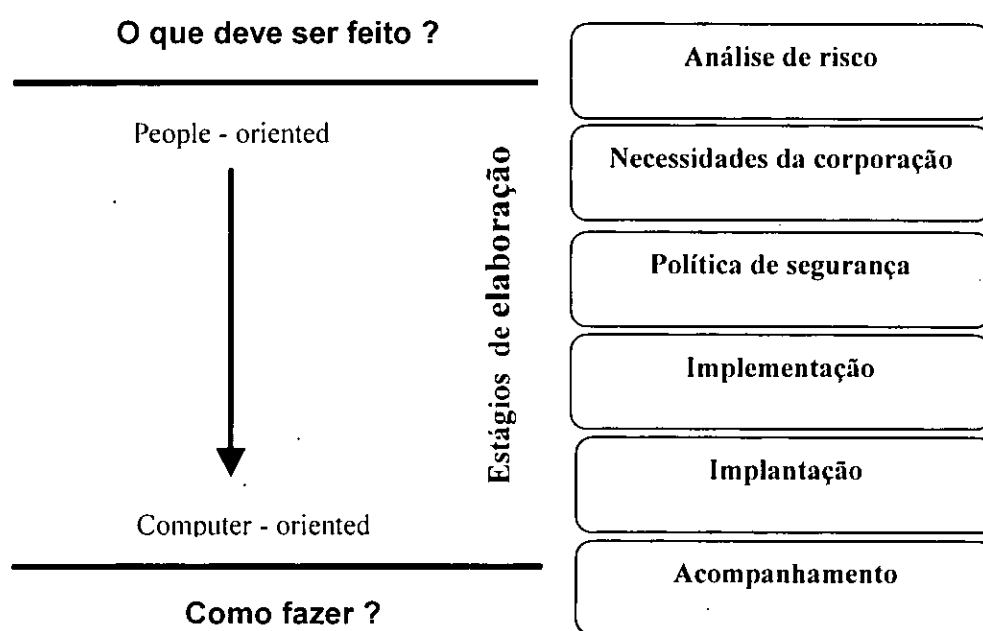


Figura II. Estrutura de um modelo de segurança

Fase de análise de risco

- A análise de risco é feita para detectar as áreas sensíveis que podem influir no sucesso ou fracasso da corporação ou nas suas iniciativas.

A análise de riscos está envolvida com a detenção dos pontos fracos e sensíveis que possam afectar a sobrevivência da corporação no caso da falha de segurança .

Um plano de controle e segurança de informações inicia-se necessariamente, por uma análise de riscos, visando direccionar os investimentos e os esforços aos sectores mais críticos e prioritários, numa situação de recursos escassos.

De modo geral, pode se dizer que cada instituição tem pontos mais sensíveis, em função do ramo de actividade que exerce. Como exemplo ilustrativo, pode se citar que as instituições do ramo comercial necessitam de preservar sua carteira de clientes e posições financeiras.

Porém esta análise não pode desprezar as diferenças existentes entre cada corporação do mesmo ramo, sendo necessária a análise criteriosa e voltada a cada situação, visando direccionar as políticas, metodologias e ferramentas, estudadas a cada caso.

A problemática de segurança de informações é ampla, uma vez que abrange não só a fuga de informações confidenciais e sigilo, mas também a integridade de informações visando sua confidencialidade e disponibilidade, bem como a sua recuperação e contingência, fazendo com que temas como incidência de vírus, existências de *backups*, redundância e planos de contingência entre outros façam parte desta análise.

De maneira pragmática, a análise de riscos passa pela seguinte sequência de acções:

- Conhecimento da actividade desempenhada pela corporação;
- Determinação de quais as informações relevantes para a actividade desempenhada e classificá-los quanto a sua natureza, a saber:
 - *Restrita*: informação que deve ficar restrita para um grupo específico de pessoas;
 - *Indispensável*: informação que deve estar sempre disponível.
- Documentação dos caminhos de fluxo de informação dentro da corporação e suas ramificações externas;
- Determinação de fontes e destinos das informações restritas e/ou indispensáveis;
- Averiguação de qual seria o impacto para a corporação se cada uma das informações restritas e/ou indispensáveis vazassem ou se perdessem de forma irrecuperável, frente a diversos cenários;

- Verificação do ponto de vista tecnológico, de quais seriam os meios técnicos pelos quais estas “catástrofes” poderiam acontecer;
- Classificação, frente a critérios de impactos, dos pontos vulneráveis.

Através desta análise de riscos em que fundamentam-se os investimentos necessários em segurança, parte-se para a fase da confecção da política de segurança.

Fase de avaliação das necessidades

- A análise das necessidades da empresa relativas á segurança de informações e definição das prioridades em função dos riscos.

Em função da análise de riscos, tem-se um quadro de todos os pontos de vulnerabilidade e de riscos associados a cada um deles. Pode-se então, traçar um quadro de necessidades de saneamento das mesmas.

Havendo escassez de recursos, deve-se avaliar as prioridades, de modo a fazer investimentos que contemplem primeiramente as iniciativas que venham ao encontro a solucionar as vulnerabilidades associadas aos maiores riscos.

Fases de projecto e desenvolvimento

O desenvolvimento de um projecto de segurança divide-se nas seguintes fases:

- *Política de segurança*: definição de uma política de segurança para a corporação como um todo e para cada área em particular;
- *Implementação*: definição de procedimentos e das ferramentas necessárias para implementar a política de segurança adoptada.

Nesta fase definem-se os processos pelos quais as vulnerabilidades serão sanadas e defini-se, também, uma política de segurança que possa congrega todas as acções de segurança dentro da mesma filosofia, fixando as directrizes básicas e prevendo, de forma pragmática, como será o mecanismo de acesso de utilizadores ás informações e todos os controles associados á manutenção da segurança como um todo.

Fase da definição de uma política de segurança

Nesta fase serão definidos todos os processos associados ao acesso de utilizadores e suas aplicações às informações, bem como os procedimentos e técnicas para a manutenção dos utilizadores de sistema, a definição dos parâmetros de segurança, identificação dos utilizadores, e principalmente, o controle de acesso aos objectos frente a política adoptada.

Implementação

A partir das definições da política de segurança, deverá ser definida a forma com que a filosofia vai-se transformar em realidade. Nesta fase, todas as ferramentas de hardware, software e administrativas terão que ser específicas, adquiridas ou desenvolvidas para que o sistema computarizado siga os procedimentos previstos na fase anterior.

Fase de implantação

- Implantação da política e configurações das eventuais ferramentas de segurança de acordo com a política adoptada;
- Promover eventuais mudanças culturais no cuidado com o tratamento das informações.

Nesta fase serão previstas as técnicas de implantação da política de segurança, pois, nas médias ou nas grandes organizações é necessário a planificação de uma norma que leve em consideração a divulgação da política de segurança, treinamento de utilizadores, a implantação em um ambiente-piloto para verificar o eventual impacto na produtividade e o acompanhamento da eficiência.

Fase de acompanhamento

- Análise dos resultados e contínua avaliação e revisão da política adoptada.

O modelo de segurança adoptado, como um todo, e a política de segurança em particular, vão sofrer um período de “amadurecimento” onde, eventualmente, serão detectados pontos que necessitam ser revistos e alterados, para aumentar a segurança, a praticidade, a produtividade ou a facilidade de administração.

Tal acompanhamento fecha o ciclo, realimentando o processo, fazendo do modelo de segurança uma acção dinâmica, sempre centrado em necessidades actuais de segurança da organização em função da dinâmica da mudança de tecnologia ou disponibilização de recursos computacionais.

Políticas de segurança

A política de segurança voltada a informática é tida como uma das fases do plano de segurança.

Trata-se de um conjunto de normas e procedimentos, automatizados ou não, que regulam como uma organização gerência, protege e distribui informações, impondo regras de acesso e, se seguidos, deverão trazer controle e segurança para as informações contidas no ambiente computacional.

Tradicionalmente, a política de segurança deve prever uma série de políticas periféricas de controle de acesso, de forma a prover serviços essenciais para o seu correcto funcionamento.

A figura III mostra os blocos que compõem uma política de segurança, enfatizando o modelo de controle de acesso a ser adoptado, visto que é o principal componente da política de segurança, pois através dele, todas as operações de acesso às informações são controladas de forma a prover segurança.

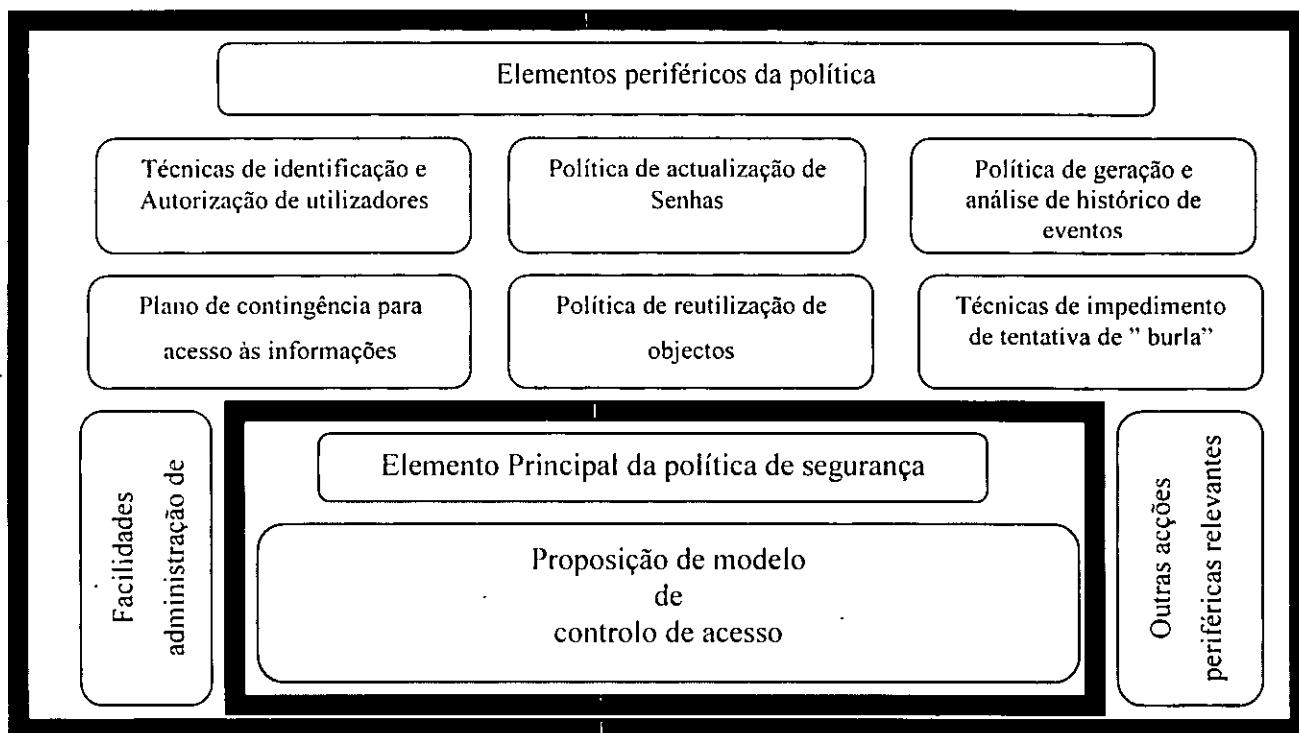


Figura III. Blocos que compõem as políticas de segurança

As directrizes fixadas no plano de segurança definirão as políticas periféricas a serem implementadas, os serviços e responsabilidades de cada uma delas e como será a interacção entre as mesmas. Porém, pode-se definir alguns mecanismos que genericamente, sempre são necessários, a saber:

Política de substituição das indetificações

- Trata-se do mecanismo de serviços relativos á substituição frequente da forma de identificar o utilizador, visando precaver-se contra eventual quebra de sigilo de senhas causada pela sua exposição e pelo conhecimento de outras pessoas em função de tempo de uso.
- Trata-se do mecanismo de serviços relativos a forçar o utilizador a usar identificações que tenham uma menor possibilidade de impedir o acesso de intrusos no sistema. No caso de uso de senhas, trata-se de um mecanismo de escolha de senhas não triviais e resistentes aos ataques externos.

Política de contingência de acesso as informações

- É um mecanismo de serviço que possibilita o acesso ao sistema, ainda que de forma segura, em situações críticas, eventualmente causadas pelo mau funcionamento deste último originado diversos motivos entre os quais um ataque.

Política de geração e análise de histórico de eventos

- Visando a existência da possibilidade de fazer uma acção preventiva e correctiva quanto a eventuais tentativas de quebra de segurança, é comum dotar os sistemas de mecanismos de segurança que possibilitem registar todos os eventos significativos (quanto a segurança) acontecidos, tais como: acesso de utilizadores aos objectos, alteração no quadro de utilizadores e seus atributos de segurança entre outros.

Política de impedimento de quebra

- São procedimentos que tem como objectivo avaliar recursividade as técnicas de quebra existentes frente ao ambiente computacional, e dotar o sistema de soluções técnicas, condições para contorná-los.

Política de facilidades de administração remota

- Trata-se prover mecanismos que possibilitam a administração da segurança de maneira remota e centralizada, favorecendo topologias de processamento descentralizado e distribuído.

ANEXOS II

ANEXOS II.1. TABELA DE FERRAMENTAS PROPOSTAS

Ferramenta	Categoria	Site
FreeBSD	Sistema operativo	http://www.Freebsd.org
AVP	Antivírus	http://www.Kaspersky.com
Gnupg	Criptografia assimétrica	http://www.gnupg.com
ModSSL	Criptografia SSL	http://www.modssl.com
Snort	IDS de rede	http://www.Snort.org
Guardian	Bloqueador de acesso	http://www.chaotic.org
Syslogng	Ferramenta de Login	http://www.Syslogng.com
VTUN	Virtual Private Network	http://www.vtun.sourceforge.net

ANEXOS III

ANEXOS III.1. CONFIGURAÇÃO DO SISTEMA OPERATIVO FREEBSD

Recompilação do Kernel

```
cp /usr/local/src/i386/conf/GENERIC \
/usr/local/src/i386/conf/BRIDGEHOST
```

Alterações em: /usr/local/src/i386/conf/BRIDGEHOST

```
ident BRIDGEHOST
maxusers 0
```

Inclusões em: /usr/local/src/i386/conf/BRIDGEHOST

```
Options IPFIREWALL
options IPFIREWALL_VERBOSE
options IPFIREWALL_VERBOSE_LIMIT=100
options IPFIREWALL_FORWARD
options IPSTEALTH
options TCPDEBUG
options RANDOM_IP_ID
options TCP_DROP_SYNFIN
options DUMMYNET
options BRIDGE
```

config BRIDGEHOST

```
cd /usr/src/sys/compile/BRIDGEHOST
make depend
make
make install
```

Assim, o *kernel* estará preparado com os recursos de filtragem de pacotes (IPFIREWALL), redireccionamento de portas (IPFIREWALL_FORWARD), redireccionamento de portas sem alteração de TTL (*Time To Live*) (IPSTEALTH), depuração de informações de cabeçalhos TCP (*Transmission Control Protocol*) (TCPDEBUG), aleatorização do campo ID de pacotes IP, ao invés de incremento por 1, (RANDOM_IP_ID), descarte de pacotes com ambos bits SYN e FIN setados (TCP_DROP_SYNFIN), *traffic shaping* (DUMMYNET) e *bridging* (BRIDGE).

Em seguida, deve-se fazer a adaptação do ficheiro de configuração global do sistema operativo (/etc/rc.conf)

Conteúdo do ficheiro /etc/rc.conf

```
hostname="bridgehost"
kern_securelevel_enable="YES"
kern_securelevel="2"
firewall_enable="YES"
firewall_type="UNKNOWN"
firewall_script="/etc/firewall"
firewall_quiet="NO"
firewall_logging="YES"
icmp_drop_redirect="YES"
icmp_log_redirect="YES"
tcp_drop_synfin="YES"
tcp_extensions="YES"
log_in_vain="YES"
inetd_enable="NO"
sendmail_enable="NO"
```

Desta forma, o sistema estará ativando um nível adequado de segurança para o *kernel*, a filtragem de pacotes e as opções avançadas de segurança, que acabaram de ser compiladas. Também, os serviços que costumam ficar ligados, como o Sendmail e o Inetd, precisam ser desativados explicitamente. Neste momento, é necessário reiniciar o sistema operacional com o comando `shutdown -r now`.

ANEXOS III.2. INSTALAÇÃO DO DETECTOR DE INTRUSOS (SNORT)

Para instalar o Snort, deve-se copiar o arquivo <http://www.snort.org/dl/snort-1.8.4.tar.gz> em `/usr/local/src/` e proceder com os seguintes comandos:

```
cd /usr/local/src/
tar xzvf snort-1.8.4.tar.gz
cd snort-1.8.4
./configure \
--prefix=/usr/local \
--exec-prefix=/usr/local \
--bindir=/usr/local/bin \
--sbindir=/usr/local/bin \
--libexecdir=/usr/local/libexec \
--datadir=/usr/local/share \
--sysconfdir=/etc/snort \
--sharedstatedir=/var \
--localstatedir=/var \
--libdir=/usr/local/lib \
--includedir=/usr/local/include \
```

```
--infodir=/usr/local/info \  
--mandir=/usr/local/man  
make  
make install
```

```
pw groupadd snort -g 100  
pw useradd snort -u 100 -g 100 -s /sbin/nologin
```

```
cd /usr/local/bin  
touch startsnort.sh  
chmod 755 startsnort.sh
```

Conteúdo do ficheiro /usr/local/bin/startsnort.sh

```
#!/bin/sh  
/usr/local/bin/snort -c /etc/snort/snort.conf -D -u snort -g snort
```

```
mkdir -p /usr/local/etc/rc.d  
cd /usr/local/etc/rc.d  
touch 00snort.sh  
chmod 755 00snort.sh
```

Conteúdo do ficheiro /usr/local/etc/rc.d/00snort.sh

```
#!/bin/sh  
echo -n ' Snort '  
case "$1" in  
start)  
/usr/local/bin/startsnort.sh  
;;  
stop)  
killall snort  
;;  
*)  
echo "Usage: `basename $0` {start|stop}" >&2  
exit 64  
;;  
esac  
exit 0
```

ANEXOS III.3. INSTALAÇÃO DO GUARDIAN

A instalação Guardian consiste nos seguintes passos:

Download do programa (<http://www.chaotic.org/guardian/guardian-1.7.tar.gz>) em `/usr/local/src/`

1. Copiar `guardian.pl`, `scripts/freebsd_block.pl` e `scripts/freebsd_unblock.sh` para `/usr/local/bin/`
2. Renomear `/usr/local/bin/freebsd_block.pl` para `/usr/local/bin/guardian_block.pl` e `/usr/local/bin/freebsd_unblock.pl` para `/usr/local/bin/guardian_unblock.pl`
3. Configurar `/etc/guardian.conf`

Conteúdo do arquivo `/etc/guardian.conf`

```
Interface r10 #Adaptador Realtek PCI
HostGatewayByte 1 #Valor do último octeto do endereço IP do gateway
LogFile /var/log/snort/guardian.log #Arquivo de log
AlertFile /var/log/snort/alert #Alertas do Snort
TargetFile /etc/guardian.target
IgnoreFile /etc/guardian.ignore
TimeLimit 300
```

5. Criar o arquivo `/etc/guardian.target` e incluir nele uma lista contendo todos endereços IP dos servidores que estão sendo protegidos pelo *bridge*.
6. Criar o arquivo `/etc/guardian.ignore` e incluir nele uma lista contendo todos endereços IP que devem ser ignorados pelo script de bloqueio automático. Esta lista deve incluir os servidores de DNS, o *gateway* padrão e demais equipamentos relevantes.

Diferente dos outros programas, o Guardian sempre precisa ser iniciado manualmente. Isto é feito com o comando `/usr/local/bin/guardian.pl`.

ANEXOS IV

ANEXOS IV. 1. ALGORÍTMO DE CHAVES SIMÉTRICAS

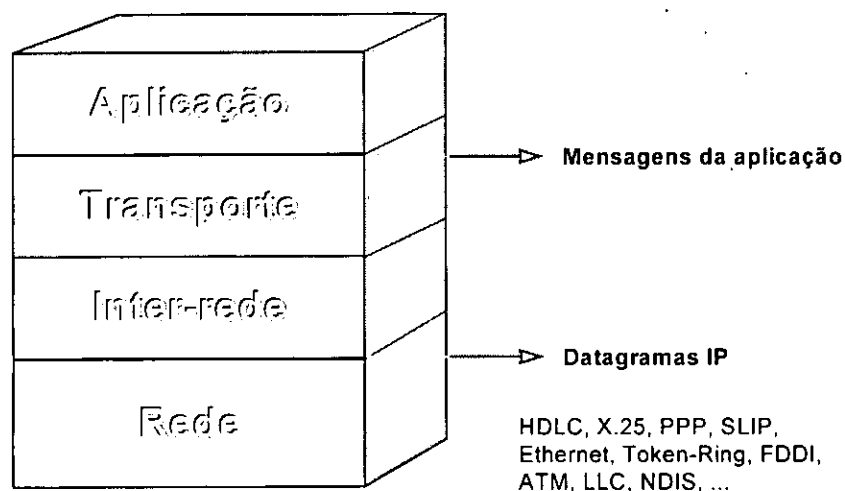
Algoritmo	Descrição
DES(Data Encryption Standart)	adoptado pelo governo da EUA desde 1977, é um dos mais conhecidos algoritmos de criptografia e usa uma chave de 56 bits.
DESX	uma modificação simples de DES em que se estabelece uma simples dupla criptografia.
Triple - DES	outra modificação em que se aplica três vezes o algoritmo DES com três chaves diferentes. Vem sendo usado ultimamente por instituições financeiras.
Blowfish	é um algoritmo rápido, compacto e simples, capaz de usar chaves de tamanho variável até 448 bits.
IDEA (International Data Encryption Algorithm)	usa chave de 128 bits e foi publicado em 1990 em Zurique na Suíça. É a base do algoritmo PGP usado em criptografia do correio electrónico.
RC2	divulgado em 1996 permite a utilização de chaves de 1 a 2048 bits.
RC4	foi divulgado em 1994 e possui chave de criptografia também de 1 a 2048 bits.
RC5	algoritmo publicado em 1994 que permite que o utilizador escolha o tamanho da chave, o tamanho do bloco a ser encriptado e o número de vezes que o dado vai ser encriptado.

ANEXOS IV.2. ALGORITMOS DE CHAVES ASSIMÉTRICAS

Algoritmo	Descrição
Deffie-Hellman	nome dado aos seus inventores paralelamente com Robert Merkle.
RSA	desenvolvido originalmente por Rivest, Shamir e Adleman (daí RSA), quando eram professores do Massachusetts Institute of Technology), pode ser usado tanto para criptografar informações quanto para servir de base para um sistema de assinatura digital.
ElGamal	baseado no sistema Deffie – Hellman e pode ser usado para assinatura digital como RSA.
DSS(Digital Signature Standart)	baseado para realização de assinatura digital, mas pode ser usado para criptografia. Actualmente usa chaves entre 512 a 1024 bits.

ANEXOS V

ANEXOS V.1. PROTOCOLO TCP/IP



ANEXOS VI

ANEXOS VI.1 QUESTIONÁRIO

Sobre o Comércio Electrónico

1) Usam Internet para que fins?

- Aprendizagem

- Consultas

- Comércio Electrónico

- Outros fins

2) Tem alguma página da sua empresa na Internet?

- Sim

- Não

a) caso sim, quais são os objectivos da sua criação?

b) Quais são as vantagens ou benefícios da sua existência?

3) Como é feito o Comércio Electrónico na sua organização?

- Via correio electrónico

- Via Internet

- Usando outros meios.

4) Na sua opinião as transações comerciais via Internet podem trazer benefícios para as empresas moçambicanas?

Avaliação de programas de segurança da informação.

1) Qual é o sistema operativo que predomina em seu(s) host(s)?

- AIX
- FreeBSD
- HP-UX
- Linux
- MacOS
- NetBSD
- Netware
- OpenBSD
- Solaris
- Windows NT/2000
- Outro

2) Sobre segurança da informação na sua rede:

(Marcar todas que se aplicam para seu caso)

- Existe uma política documentada, que estipula limites e penalidades.
- Faz recomendações verbais e informais para os utilizadores da rede.
- Não existe nada nesse sentido.

3) Quais dos conceitos de segurança aplica na rede que administra?

(Marcar todas que se aplicam para seu caso)

- Bridging (*Firewall* dedicado sem camada IP configurada)
- Centralização de autenticação: NIS LDAP Outro
- Criptografia em terminais remotos (Secure Shell, SSLTelnnet...)
- DMZ (Isolamento físico e lógico da rede de servidores)
- Filtragem de pacotes

4) Sobre a filtragem de pacotes...

(Marcar 1 opção)

- Tenho um (ou mais de um) host fazendo somente filtragem de pacotes.
- Mantenho um filtro de pacotes mas agrego nele outras funções(proxy, Nat, Ftp etc...)
- Configuro a filtragem de pacotes em cada servidor que mantenho.
- Todos serviços que disponibilizamos estão em um computador e nele filtro pacotes.
- Não faço filtragem de pacotes

5) Se não mantém um host dedicado somente a filtrar pacotes, isto acontece por que motivo:

(Marcar todas que se aplicam para seu caso)

- Não aumentará segurança no meu caso.
- Não consigo conciliar uma tarefa desta complexidade com meu tempo disponível.
- Não é financeiramente inviável.
- Não sei como fazer.

6) Quais dos sistemas de detecção de intrusos mantém efectivamente em sua rede:

(Marcar todas que se aplicam para seu caso)

- AAFID
- Aide
- Bro
- Chkrootkit
- Logcheck
- Netsaint
- Ngrep
- Portsentry
- Snort
- Tcpdump

- Tripwire

- Outros.

- Nenhum.

7) Dentre os ataques listados abaixo, quais já detectou em sua rede?

(Marcar todas que se aplicam para seu caso)

- Alteração do conteúdo servidor Web

- Ataque contra utilizadores da sua rede

- Negação de serviço

- Força bruta contra alguma conta no sistema (POP, FTP etc...)

- Varredura de portas (*port scan*)

- Tentativas de obter mapas de DNS

- Outros

- Nenhum