TRABALHO DE INVESTIGAÇÃO

Segurança na Internet : *Políticas e Firewall*

Autor: Mário Jorge Honwana
Supervisor: dr. Paulo Maculuve
Co-Supervisor: Drª. Esselina Macome

Maio de 2002

Agradecimentos

Os especiais agradecimentos à todos que contribuíram directa ou indirectamente para a elaboração deste trabalho:

Ao meus supervisores, dr. Paulo Maculuve e Drª. Esselina Macome, pelo apoio prestado , empenhando todo o seu conhecimento e experiência na orientação deste trabalho.

Ao Eng. Rogério Lam pela assistência e apoio técnico que me proporcionou na realização do trabalho.

A todos os amigos e colegas do BCI que sempre estiveram disponíveis a opinar e criticar.

Finalmente, um agradecimento especial aos meus pais e irmãos, sem o apoio dos quais jamais teria sido possível realizar os meus estudos.

Declaração de honra

"Declaro que este trabalho é resultado das minhas próprias investigações e o mesmo foi realizado apenas para ser submetido como trabalho de Licenciatura em Informática na Universidade Eduardo Mondlane"

Maputo, Maio de 2002

_____

(Mário Jorge Honwana)

RESUMO

A elaboração de politicas de segurança no contexto da *Internet* pressupõe um conhecimento profundo de diversos mecanismos relacionados com o funcionamento de redes informáticas e dos intervenientes nos processos de comunicação através das mesmas.

O presente trabalho aborda aspectos essenciais de segurança na *internet*, como os serviços existentes na *internet*, suas vulnerabilidades; Tipo de atacantes à sistemas informáticos e formas de ataques; Formas e estratégias de protecção dos sistemas contra as várias formas de ataques conhecidas.

Estes conhecimentos permitiram, numa segunda fase do trabalho, elaborar uma proposta de política de segurança para a *Internet* do Banco Comercial e de Investimentos (BCI) e a construção de um *firewall* que implementando tais politicas garante a segurança do sistema em estudo(caso de estudo).

Para a elaboração do trabalho, foi necessário realizar consultas à bibliografia (e a páginas de *Internet)* relacionada com Segurança de sistemas informáticos e *Internet*; entrevistas com especialistas na área , com os administradores do sistema informático e da direcção do BCI.

Foi tomada em consideração a realidade actual do Banco em termos dos serviços disponíveis aos seus utilizadores, as necessidades de expansão em termos físicos da rede informática e da expansão em termos comerciais dos serviços a disponibilizar aos clientes por via da *Internet.*

O resultado do trabalho, foi a elaboração de um proposta de política de segurança para o sistema informático do Banco Comercial e de Investimentos e a construção de um *Firewall* que implementando tal politica, se propõe proteger o sistema de situações de risco resultantes de uma ligação à *Internet.*

ÍNDICE

INTRODUÇÃO

A *Internet* tem crescido a um ritmo bastante acelerado nos últimos anos. Ela passou a ser um "objecto" indispensável ao quotidiano de milhares de pessoas e organizações em todo o mundo, permitindo encurtar distancias, eliminar fronteiras, economizar tempo e dinheiro. Ter uma ligação à *Internet* é cada vez menos uma questão de opção e passa a ser uma necessidade indispensável à sobrevivência de muitas organizações. Os custos de distribuição de produtos e serviços das organizações podem ser drasticamente reduzidos.

Os computadores ligados a *Internet* são vulneráveis. Eles podem e têm sido comprometidos no seu funcionamento. Quanto maior for o número de propósitos para os quais a *Internet* for usada, mais informação valiosa as organizações colocam *on-line* , mais pessoas a utilizam e mais convidativos a acções criminosas estes computadores se tornam.

Assim, segurança constitui um factor determinante na implementação de qualquer sistema informático com acesso à *Internet* . Diversos factores podem contribuir para comprometer o normal funcionamento dos sistemas. A *internet* é uma rede de duas vias; da mesma forma que torna possível aos servidores publicarem informação para milhares de utilizadores, também possibilita que pessoas mal intencionadas, violem os computadores na rede onde os serviços estão sendo executados.

A segurança na *Internet* requer uma atenção especial por diversos motivos, destacando-se os seguintes:

-O facto de estar a ser cada vez mais usada por empresas, governos e outras instituições para a disseminação de informação importante e realização de transacções comercias . Reputações podem ser prejudicadas e muito dinheiro pode ser perdido se os servidores de *Internet* estiverem sujeitos a riscos.

- Uma vez quebrada a segurança, *navegadores* e *servidores* podem ser usados por *crackers* (pessoas que invadem sistemas, com más intenções) como base para desferir mais ataques contra outros usuários e organização.

- Ser consideravelmente mais caro e demorado resolver um incidente de segurança do que tomar medidas preventivas.

O Banco Comercial e de Investimentos (BCI), fundado em 1997, é uma instituição financeira que tem como principais actividades a angariação de poupanças e a concessão de créditos para diversos fins. Tem a sua sede em Maputo e possui agências na Beira, Nampula, Nacala, Chimoio, Tete, Pemba, Xai-Xai, Chokwé e Quelimane prevendo-se que até ao final do ano 2002 tenha balcões nas restantes províncias. Todos os balcões do BCI funcionam em *on-line* ,numa arquitectura *cliente- servidor* .

Para além de serviços bancários, estão igualmente disponíveis aos utilizadores da rede o serviço básico de *Internet* e o correio electrónico.

Estes e outros serviços podem estar sujeitos a vários tipos de ataques vindos do exterior que prejudicariam seriamente o normal funcionamento do banco. O correio electrónico recebido pela *Internet* constitui uma fonte bastante grande de disseminação de vírus que podem criar graves problemas. Ataques

de *intrusão* (tipo de ataque na *Internet* que permite que o *hacker* tenha um controle remoto de computadores dentro de uma rede à qual não era suposto ter acesso) podem também ser efectuados com vários objectivos como sejam a destruição de informação, espionagem comercial, fraudes entre outros que podem resultar em desfalques. Podem, também, pessoas mal intencionadas tentar interceptar o correio electrónico com o objectivo de aceder a informação confidencial.

Pelos motivos acima expostos e porque existe a médio prazo um projecto de implementação de *homebanking* , usando tecnologia *Web* ,o que constituiria mais uma potencial fonte de atracção de indivíduos maliciosos à pratica de actividades ilícitas, é necessário dotar o BCI de uma estrutura que o permita uma redução máxima dos riscos de sofrer ataques via *Internet.*

A segurança de sistemas informáticos deve ser vista sob diversas perspectivas. No presente trabalho, a questão da segurança será abordada apenas sob o ponto de vista da *Internet.*

A metodologia usada no trabalho consistiu na revisão bibliográfica de material sobre Segurança e Comércio electrónico, pesquisas de páginas de *Internet* e entrevistas com especialistas em áreas relacionadas com o tema do trabalho.

O presente trabalho tem como objectivo propor uma política de segurança para o BCI de acordo com as suas necessidades e prioridades e com base nestas políticas construir e implementar um *firewall* . Para tal, foi necessário identificar:

- todos os serviços que neste momento estão disponíveis aos utilizadores da rede;

- os outros serviços que o banco pretende (ou pode) disponibilizar aos seus utilizadores a curto e médio prazo;

- os riscos que estes serviços podem representar em termos de segurança ;

- as formas actualmente conhecidas de combater esses riscos.

Estes objectivos têm em vista garantir a confidencialidade e integridade da informação.

O trabalho encontra-se organizado em 6 capítulos: Os conceitos relacionados com segurança (capítulos I a IV), um caso de estudo em que são aplicados tais conceitos (Capitulo V) e Conclusões (Capitulo VI).

O capítulo I, descreve os principais intervenientes no contexto da segurança na *Internet.* Assim, é visto o "objecto" que se pretende proteger, o que representa perigo para um sistema : tipos de ataques, de atacantes e as suas formas de actuação. são também vistos neste capítulo os serviços de *Internet* mais conhecidos actualmente , suas características, pontos fortes e vulnerabilidades.

O capítulo II, descreve algumas técnicas de protecção de sistemas e da informação que circula na *Internet*, com maior realce para o uso de *Firewalls* e da Criptografia.

O capítulo III, apresenta a forma como deve ser concebida uma política de segurança . São discutidas algumas estratégias de segurança a implementar.

O capítulo IV, analisa as medidas a adoptar quando um ataque é realizado com sucesso. São discutidas as formas de detectar ataques , atacantes e o modo de recuperar do ataque sofrido.

Capitulo V, é o caso de estudo. Criação da política de segurança do sistema informático do BCI e a construção de um *Firewall* que materialize tal politica, são as principais matérias do capítulo.

No capítulo VI, são apresentadas as conclusões e recomendações do trabalho.

CAPÍTULO I

PRINCIPAIS INTERVENIENTES NO ÂMBITO DA SEGURANÇA

O objectivo do presente capítulo é identificar e descrever os principais intervenientes no processo de segurança de sistemas informáticos ligados à *Internet.*

1.1 O OBJECTO A PROTEGER

Segundo *Chapman and Zwicky* (1995) uma ligação à *Internet* levanta três tipos de riscos:

- Sobre os dados.
- Sobre os recursos da rede.
- Sobre a reputação das instituições.

Quando se elabora um projecto de segurança, é necessário clarificar em primeiro lugar o que se pretende proteger:

OS DADOS

O principal objectivo ao se pensar em segurança de sistemas informáticos é proteger a informação, que é o elemento mais valioso em tais sistemas.

A informação existente nos sistemas de informação deve possuir três características (Chapman and Zwicky,1995):

CONFIDENCIALIDADE – Protecção da informação de modo a que esta não seja revelada a pessoas não autorizadas. Uma instituição como o BCI possui muita informação que se pretende que seja apenas do conhecimento interno e dos seus clientes, tais como os saldos dos clientes, créditos, entre outros. Para além disso existe a informação sobre as políticas e estratégias de acção do ponto de vista do negócio.

INTEGRIDADE – Protecção da informação de modo que esta não seja alterada por indivíduos não autorizados. A informação armazenada nos computadores não deve, em circunstancia alguma, ser alterada por pessoas estranhas à actividade da instituição. Alterações a registos como os de saldos de clientes, podem resultar em elevadas perdas financeiras.

DISPONIBILIDADE – A informação deve estar disponível sempre que dela se necessitar. De pouco adianta a informação estar armazenada qúando não se pode a ela aceder sempre que se necessita. Os clientes devem poder obter todas as informações que sejam do seu interesse, sempre que tal seja necessário.

OS RECURSOS COMPUTACIONAIS

Os recursos necessários para a implementação de uma rede informática também devem ser alvo de uma atenção especial na elaboração de politicas de segurança. Um ataque bem sucedido , à uma rede informática pode ter consequências muito graves, pois pode resultar na paralisação ou danificação dos recursos desta.

O ataque pode resultar por exemplo, na ocupação do espaço livre do disco de um computador ,de tal modo que não seja possível armazenar mais informação, ou então um caso mais grave que provoque o bloqueio do próprio computador.

Para o caso de uma instituição como o BCI, o bloqueio do seu servidor central pode provocar a paralisação quase geral das actividades, criando grandes transtornos aos clientes que se verão impossibilitados de movimentar o seu próprio dinheiro e por consequência prejuízos incalculáveis poderão recair sobre a instituição.

A REPUTAÇÃO

Vivendo numa economia de mercado onde a qualidade da prestação de serviços pode determinar vantagens sobre a concorrência e muitas vezes a capacidade de uma empresa se impor ou mesmo sobreviver, um ataque pela *Internet* bem sucedido pode ter consequências irreparáveis sob o ponto de vista da reputação de uma instituição. Os clientes poderão perder a confiança que nela depositam.

Para o caso de uma instituição que tenha uma página na *Internet*, a sua reputação pode ficar afectada por diversas formas:

- O atacante pode apenas pretender chamar a atenção e mostrar a vulnerabilidade do *site*.

- O *site* pode ser usado como base para realizar novos ataques à outros *sites*, ficando o verdadeiro atacante encoberto. A responsabilidade do ataque seria então imputada à uma organização que por sua vez também terá sido vítima de um ataque.

- A partir deste *site* podem ser publicados outros *sites* (piratas) que façam, por ex., a venda ilegal de programas informáticos , material pornográfico ou outro tipo serviços inadequados.

As instituições bancárias preocupam-se sempre em passar para o exterior (como forma de ganhar mais clientes) uma imagem de seriedade, solidez e transparência que ficariam bastante afectadas se verificasse um ataque desta natureza.

1.2 O QUE REPRESENTA PERIGO ?

Para se poder elaborar uma estratégia de segurança eficiente, é necessário conhecer-se bem os riscos a que se está exposto ao se conectar uma rede informática à *Internet*.

1.2.1 TIPOS DE ATAQUES

Existem vários tipos de ataques perpetrados por *hackers* da *Internet*. Estes ataques podem atingir qualquer ponto da rede e os serviços disponíveis. Alguns destes são desenhados com o objectivo final de conseguir o acesso às máquinas. Outros têm o objectivo de impedir que legítimos usuários tenham acesso aos serviços que pretendem, ou provocar danos nos computadores atacados. Segundo *Larson & Stephens(2000)*, os principais tipos de ataques, são:

VÍRUS

O mais conhecido tipo de ataque à um sistema é o *vírus*. Um *vírus* informático obtém esse nome pela forma como se propaga no sistema. Tal como nos humanos, os computadores são contaminados com *vírus* ao interagirem com outros computadores que estejam infectados por *vírus*.

Um *vírus* é um programa informático que tem como resultado da sua acção a ocorrência de um dano ao sistema (geralmente consiste na eliminação de ficheiros ou formatação de discos). Os *vírus* geralmente acoplam-se à outros programas ou ficheiros , que ao serem executados (são lidos para a memória) este também é lido. Uma vez instalado na memória realiza duas acções:

- A acção para a qual foi desenhado: formatar o disco duro, eliminar ficheiros, exibir mensagens, entre outros.

- Acoplar-se a outros programas, de modo a infecta-los também.

Os programas então infectados podem depois ser enviados via *e-mail* (correio electrónico) infectando outras máquinas. Deste modo o *vírus* vai-se propagando.

WORM

Este é um tipo de ataque muitas vezes confundido com o *vírus*. De facto, possui um comportamento bastante similar ao de um *vírus*, uma vez que o seu objectivo final é de comprometer a segurança de múltiplas máquinas por auto-propagação. A diferença esta na maneira como cada um se propaga. Enquanto um *vírus* se acopla à programas já existentes, um *worm* contem ele próprio um programa ou parte dele, que quando executado realiza as duas acções de um *vírus* (destruição e propagação). Se um *worm* fizer um ataque bem sucedido , ele então copia-se a si próprio para o computador afectado, continuando o ciclo desta forma.

TROJAN HORSE (CAVALO DE TROIA)

Outro tipo de ataque bastante frequente é o *Trojan Horse* .Este nome foi dado em homenagem ao povo de Tróia, pelos Gregos, durante a guerra de Tróia. Após várias tentativas fracassadas de tomar a cidade de Tróia, os Gregos decidiram esconder-se dentro de um grande cavalo de pedra e deixaram-no às portas da cidade. Os cidadãos de Tróia, convencidos que se tratava de um presente dos deuses, levaram-no para o interior da cidade. Uma vez dentro da cidade, as tropas Gregas saltaram para fora do cavalo e atacaram com sucesso.

Trojan Horse é um programa desenhado por *hackers* que aparenta realizar uma acção absolutamente normal, mas que tem um segundo propósito. Enquanto executa a acção visível, o *Trojan Horse* realiza, por trás, outros comandos que não têm relação nenhuma com a sua acção primária sem que seja possível notar, provocando danos ao sistema.

NEGAÇÃO DE SERVIÇOS

Nem todos os atacantes têm como objectivo tomar o controle ou provocar danos ao sistema. A negação de serviços é um tipo de ataque em que o objectivo é impedir que legítimos usuários do sistema tenham acesso aos seus serviços, fazendo com que estes estejam indisponíveis.

Este tipo de ataque ocorre com mais frequência nas páginas da *Web* , quando o atacante faz milhares de pedidos (simultâneos) de acesso a um terminado *site* , provocando a saturação do sistema , que não consegue responder a todos os pedidos que lhe chegam. Deste modo, os utilizadores que realmente pretende consultar a referida página, não o conseguem fazer.

SPOOFING (ENGANAR)

Este é um tipo de ataque em que o *hacker* se faz passar por outra pessoa, i.e, assume identidade alheia. Existem várias formas de realizar este ataque. O *SPOOF* (enganar) pode ser realizado sobre um *e-mail* de tal modo que este aparente ter sido enviado por outro utilizador. Pode-se também fazer o *SPOOF* de um endereço IP de tal modo que os dados aparentem estar a ser enviados por uma máquina diferente. Nas paginas da *Web* este ataque é também possível, resultando que o utilizador pode estar a consultar uma página que provem de um determinado *site* diferente daquele que pensa realmente estar a consultar.

A técnica de *SPOOFING* tem sido bastante usada por *hackers* e muitas vezes em combinação com outros tipos de ataques. De facto, qualquer indivíduo que realize um ataque a um sistema não pretende deixar um rasto, e de preferência procura encobrir a sua identidade.

SNIFFERS

Sniffers são dispositivos que capturam pacotes de redes. O seu propósito legítimo é analisar o tráfego de uma rede e identificar áreas potenciais de preocupação. Estes são sempre uma combinação de *software* e *hardware,* que faz a captura de pacotes de rede. Os *sniffers* constituem alto nível de risco, pois podem ser usados para:

- capturar as senhas secretas dos utilizadores do sistema;

- capturar informações confidenciais;

- abrir brechas na segurança do sistema, ou ganhar acessos de alto nível.

A existência de um *sniffer* não autorizado pode indicar que o sistema já esteja comprometido. Os ataques de *sniffers* são comuns, principalmente na *Internet*. Um *sniffer* bem colocado pode decifrar centenas de senhas em algumas horas.

Nem todos os ataques à sistemas resultam de técnicas concebidas por *hackers*. Alguns resultam de aproveitamento de erros e/ou deficiência de programas (*bugs)* usados no sistema. Os piratas informáticos estão sempre em busca destes erros que muitas vezes deixam "buracos" por onde depois são executados os ataques aos sistemas.

1.2.2 TIPOS DE ATACANTES

Existem várias formas de classificar os atacantes de sistemas, mas todos eles possuem um certo número de características muito próprias. Com base nessas características é possível dividi-los em grupos: espiões, curiosos e os simples destruidores (vândalos). Segundo *Chapman & Zwicky(1995)* os principais tipos de atacantes são:

VÂNDALOS

Os vândalos são o tipo de atacante que têm como objectivo provocar destruição e danos aos sistemas, sendo os seus actos e consequências imediatamente visíveis. Este é o tipo de atacante que não se preocupa muito em ocultar os seus actos e cuja acção circunscreve-se a um espaço de tempo muito curto, uma vez que estes são facilmente detectados.

JOYRIDERS

Este é o tipo de atacante basicamente curioso e sem intenções maldosas. Ele invade por pensar que o sistema atacado pode conter informação que lhe possa interessar, por simples diversão, ou ainda por um espírito de diversão. São geralmente o tipo de pessoas que tentam encontrar uma maneira diferente de passar o seu tempo. Mas muitas vezes, estes podem também provocar danos aos sistemas, por ignorância ou por tentativa de encobrir os seus actos. Os *Joyriders* são geralmente atraídos por *sites* muito populares ou por sistemas que possuam computadores pouco comuns.

ACUMULADORES DE RECORDES

Este é o tipo de atacante cuja competição entre si está na base da sua motivação de acção, tentando contabilizar o número e tipo de sistemas que conseguem violar. Invadir um sistema com um grau de dificuldade elevado constitui um desafio e um teste às suas capacidades. Porém, este é o tipo de atacante que tenta violar todo o *site* que puder. A quantidade de vítimas é para ele tão importante quanto a qualidade, mas tal como os *Joyriders* e os Vândalos, estes preferem *sites* que tenham algum particular interesse.

Em todo o caso, este é também um tipo de ataque que pode provocar danos. Os atacantes guardam sempre informação sobre o sistema atacado, usando-a possivelmente como referencia para novos ataques e se possível usam as máquinas deste sistema para atacar outros sistemas.

Este é um tipo de atacante que geralmente só é descoberto muito tempo depois de conseguir "furar" um sistema.

ESPIÕES

Muitas das pessoas que violam sistemas fazem-no pelo simples facto deles existirem. Os espiões habitualmente apoderam-se de informação que possa ser directamente convertida em dinheiro. Se descobrem algum segredo procuram vendê-lo, apesar de este não ser o seu negócio principal.

A grande espionagem computacional é mais rara fora dos meios tradicionais de espionagem. Esta é bem mais difícil de detectar, pois um atacante que invada um sistema e se limite a copiar ficheiros, nunca mais voltando a violar o sistema dificilmente pode ser detectado.

Em termos práticos, a maioria das organizações não consegue impedir que espiões sejam bem sucedidos. As precauções que os governos e as grandes companhias tomam para proteger a informação, são complexas e caras, sendo por este motivo apenas usadas em recursos críticos.

IGNORANTES E DESCUIDADOS

Muitos dos desastres que acontecem não são intencionalmente causados. Eles surgem por ignorância dos utilizadores ou por mero acidente. Um estudo revela que cerca de 55% dos incidentes de segurança são causados por utilizadores pouco habilitados que tentam fazer algo sem saberem o que de facto estão a fazer.

É muito frequente organizações destruirem a sua própria informação ou publicarem-na por engano. Os sistemas de segurança não podem proteger contra este tipo de situações , não existindo deste modo nenhuma forma eficiente de combater estas situações.

1.3 SERVIÇOS DE INTERNET

Existe um grande número de serviços que os utilizadores geralmente pretendem ter disponíveis ao se ligarem à uma rede de *Internet.* Contudo, é necessário estar atento aos potenciais problemas de segurança que tais serviços possam levantar.

De seguida são descritos alguns dos serviços de *Internet* mais conhecidos actualmente:

CORREIO ELECTRÓNICO

O correio electrónico (*e-mail*) é o serviço mais popular e básico de rede. Fragilidades na protecção do *e-mail* podem permitir dois tipos de ataques: contra a reputação da instituição e ataques de manipulação social (ex. O tipo de ataques em que os utilizadores recebem *mails* aparentemente vindo do administrador da rede, instruindo-os a mudar as suas *passwords* para uma outra). A recepção de *e-mail* ocupa espaço e tempo do computador, sujeitando este a ataques de negação de serviços, apesar de, com uma configuração própria, só os serviços de *e-mail* virem a ficar afectados. Particularmente com modernos serviços de multimédia de correio electrónico, podem ser enviadas mensagens que contenham programas que corram sem que possam ser devidamente supervisionados, acontecendo muitas vezes ataques de *Trojan Horses.*

Na prática, o problema mais frequente relacionado com o correio electrónico (c.e) está ligado as *bombas de correio electrónico.* Uma bomba tradicional de correio electrónico é uma série de mensagens (talvez milhares) enviadas para uma determinada caixa de correio. O objectivo do ataque é inundar a caixa receptora de mensagens sem qualquer utilidade.

O tamanho médio de uma bomba de correio é de aproximadamente 2 MB. (*Larson & Stephens,2000*)

Existem programas (pacotes de bombas de c.e) que automatizam o processo de envio de envio das bombas. É importante que os administradores dos sistemas conheçam tais pacotes e os nomes dos arquivos associados.(Anexos 1 e 2)

A forma mais eficiente de combater tais ataques é através de esquemas de exclusão ou filtros de correio. Utilizando tais ferramentas, é possível rejeitar correio com tais características. (*Chapman & Zwicky,1995*)

TRANSFERÊNCIA DE FICHEIROS

Os protocolos de transferência de dados de *c.e* foram desenhados para lidar com pequenos ficheiros, em formato legível por humanos. Estes protocolos podem executar alterações em tais mensagens, mas o mesmo já não podem fazer quando se trata de programas. Actualmente os protocolos de *c.e* possuem alternativas que permitem que ficheiros binários, grandes, possam ser repartidos em pequenos sub-ficheiros e depois codificados do lado de quem envia, descodificados e reagrupados do lado de quem recebe.

Os utilizadores da rede podem pretender procurar os ficheiros que desejam, em vez de aguardarem que alguém os envie. Nestes casos, mesmo estando disponível o *mail,* é útil ter um método desenhado para a transferência de dados.

File Transfer Protocol (FTP) é o protocolo *standard* da *Internet* para este propósito. Teoricamente, autorizar que os utilizadores recebam ficheiros do exterior não representa um acréscimo de risco em relação ao *e-mail*. De facto, existem *sites* que oferecem serviços autorizando o acesso ao FTP via *c.e*. Mas geralmente os usuários realizam mais transferências de ficheiros quando o próprio FTP está disponível.

Neste caso existem maiores riscos de serem recebidos programas e dados não desejáveis. O que torna um programa não desejável é, em primeiro plano, o receio de que este possa ser um *Trojan Horse*. No entanto, actualmente as maiores preocupações são relativas ao facto de os utilizadores poderem, eventualmente, transferir material como *software* pirata, jogos de computadores e imagens que ocupam muito espaço do disco.

O reverso da moeda dá-se quando se autoriza outros utilizadores a fazer FTP para dentro da rede, o que é muito mais arriscado. Um FTP anónimo é um mecanismo extremamente popular de conceder a utilizadores remotos, acesso a ficheiros sem ser preciso conceder acesso total à máquina. Se for executado um *servidor* FTP, pode-se permitir que utilizadores acedam a ficheiros armazenados numa determinada área pública do sistema, sem ser necessário conceder permissão de uso dos restantes recursos do sistema.

Ao se instalar um *servidor* de FTP anónimo, é necessário assegurar que os utilizadores que beneficiam deste serviço não terão acesso à outras áreas ou ficheiros do sistema e é necessário, também, garantir que os utilizadores não usem o *servidor* de forma inapropriada. (*Larson & Stephens,2000)*

ACESSO REMOTO E EXECUÇÃO DE COMANDOS

Os programas que providenciam um acesso remoto aos computadores permitem o uso de um sistema remoto como se fosse um terminal conectado directamente.

TELNET é o serviço *standard* para o acesso remoto na *Internet*. Este permite que o acesso se efectue sem necessitar de muitas exigências técnicas. Já foi considerado um serviço seguro, pois exige a autenticação dos utilizadores. Mas, infelizmente, este serviço envia todas a sua informação sem que esteja encriptada, o que o torna bastante vulnerável à ataques. Actualmente é considerado um dos serviços mais perigosos para o uso em acesso remoto. A preocupação com a segurança deve sempre recair no lado de quem autoriza o acesso remoto ao seu sistema.

TELNET só é seguro se a máquina remota e todas as redes entre esta e a máquina local forem seguras. Isto significa que este não é seguro para ser usado na *Internet*, pois aí nunca é possível identificar todas as redes intervenientes e muito menos depositar confiança nelas. Este serviço pode ser útil como um mecanismo de acesso remoto, se os utilizadores viajam muito e têm sempre disponíveis *sites* ligados à *Internet*.(*Champman & Zwicky,1995)*

NOTÍCIAS DE INTERNET

Enquanto o correio electrónico permite que pessoas se comuniquem através de mensagens trocadas entre dois utilizadores ou um grupo de utilizadores inscritos numa lista de pessoas interessadas num determinado tópico, os grupos de notícias são boletins de notícias difundidas pela *Internet*, desenhados para comunicações *muitos-para-muitos.*

Os riscos que estas notícias representam, são semelhantes aos do correio electrónico. Os utilizadores podem inadvertidamente confiar na informação que recebem. Podem enviar informação confidencial e podem também receber *floods.*

Network News Transfer Protocol (NNTP) é o protocolo usado para transferir noticias pela *Internet*. Ao se configurar um *servidor* de notícias, é necessário determinar o modo mais seguro de estas serem encaminhadas pelo sistema, de maneira que *NNTP* não possa ser usado para realizar ataques ao sistema. (*Chapman & Zwicky,1995*)

WORLD WIDE WEB

O correio electrónico, *FTP, TELNET,* e as notícias de *Internet* existem desde os primeiros tempos da *Internet.* O *WWW* é um novo conceito totalmente baseado na *Internet* que funciona em parte com base em alguns serviços já abordados e também com base no novo protocolo *Hypertext Transfer Protocol (HTTP). WWW* é uma colecção de servidores de *HTTP* na *Internet.*

A *Web* é a responsável pela grande explosão na actividade da *Internet* nos últimos anos. Esta usa tecnologia *hypertext* para fazer a ligação entre documentos de diferentes formatos que podem incluir textos, imagens gráficas, ficheiros de sons e de vídeo. O *hypertext* providencia as condições para se navegar de um documento para outro. Os utilizadores podem mover-se facilmente entre páginas , independentemente da localização destas, bastando para isso que seleccionem a palavra ou figura para a qual a ligação *http* tenha sido definida.

O formato mais comum de ficheiros da *Web* é o *HyperText Markup Language (HTML)*, que é uma linguagem padronizada para descrição de páginas de *Web.* Fornece capacidades básicas de formatação de documentos, incluindo a capacidade de adicionar gráficos. Permite também, que sejam adicionadas ligações para outros *servidores* e ficheiros.

Os *Web browsers* (navegadores de *Internet*) são bastante populares, pois disponibilizam um *interface* gráfico muito rico para um imenso número de recursos. Informação que em tempos remotos não estava facilmente disponível, ou que só podia ser acedida por *experts* informáticos, é agora facilmente acedida. A Grande utilidade da *Web* deve-se em grande parte à sua flexibilidade. Infelizmente, os *Web Browsers* e os *servidores* de *Internet* são dificeis de manter seguros. Do mesmo modo que passou a ser mais fácil transferir ficheiros ou programas através destes que por *FTP,* também se tornou mais simples transferir e executar programas maliciosos.

Porque um documento *HTML* pode ligar-se facilmente à outros *sites*, os utilizadores podem sentir-se confusos sobre a "paternidade" dos documentos a que acedem. Tais utilizadores poderão não se aperceber quando transitam de um documento do *site* interno da sua organização, para um documento de um *site* externo. Esta situação pode ter duas consequências graves:

- Os utilizadores podem confiar, inadvertidamente, em documentos externos. Este é o lado perigoso de existirem transições suaves entre *sites*.

- Os utilizadores podem responsabilizar os administradores dos seus sistemas, por danos causados por terceiros.(*Chapman & Zwicky,1995*)

SERVIÇOS DE INFORMAÇÃO

A *Internet* não possui um serviço adequado para se realizarem pesquisas sobre informações pessoais dos seus utilizadores. No entanto, algumas tentativas de se fazer este tipo de serviços já surgiram. Mesmo que, se conheça o verdadeiro nome e o local de trabalho da pessoa em questão, não existe nenhum lugar centralizado onde se possa obter o seu *username* e endereço de *e-mail.* Com o objectivo de minimizar esta lacuna, foram criados dois serviços: *Finger* e o *whois.*

O *finger* procura informação sobre o utilizador que tenha um *acount* na máquina onde se faz a pesquisa, quer este esteja activo, quer não. Esta informação pode incluir dados pessoais do utilizador, localização dos seus escritórios, informação sobre as últimas vezes que acedeu ao sistema e alguma breve mensagem especificada por este.

Não é necessário conhecer o nome completo do utilizador para se poder usar o *finger.* Este indica sempre a lista de todos os utilizadores cujos nomes ou *username* contenha o *string* indicado. Caso não tenha sido indicado nenhum, então serão listados todos os utilizadores activos naquele momento.

O *whois* é um serviço similar ao *finger,* mas apenas disponibiliza informação sobre *hosts*, domínios e seus administradores. Por defeito, este serviço pesquisa a informação no *hot* rs.internic.net no *INTERNIC* (Internet Networks Information Centre) que dispõe de informação sobre domínios de *Internet* e administradores de redes.(*Chapman & Zwicky,1995*)

SERVIÇOS DE CONFERENCIAS EM TEMPO REAL

Existem vários serviços de conferências em tempo-real, sendo o *Talk, Irc* e os serviços de *MBONE* os mais conhecidos. Todos estes serviços garantem condições necessárias à comunicação em tempo-real. Enquanto correio electrónico e as noticias de *Internet* são concebidos para facilitar comunicação assíncrona, funcionando mesmo que os intervenientes não tenham acedido ao sistema, por seu turno as conferencias tempo-real são desenhadas para uso interactivo em *on-line.*

O *Talk* é o sistema de conferência mais antigo usado na *Internet.* Esta disponível em quase todas máquinas *Unix* e permite que dois utilizadores estabeleçam comunicação. Não é muito usado entre pessoas que não se conheçam, sendo geralmente amigos ou colegas de serviço quem faz uso deste serviço.

É muito difícil garantir a utilização deste serviço através de um *firewall*, sem que se abram brechas na segurança da rede. Daí que o seu uso seja geralmente autorizado, apenas, a nível interno da rede.

O *Internet Relay Chat* (IRC) tem a sua própria cultura, envolvendo muitas pessoas conversando umas com as outras. Os utilizadores acedem a este serviço através de *clientes* dedicados de IRC ou usando o *Telnet* para aceder a um *site* que providencie serviços de clientes de IRC. Ao contrário do *Talk*, que limita a conversação a um par de utilizadores, o IRC permite que um número ilimitado de utilizadores converse simultaneamente.

Existem vários tipos de problemas segurança relacionados com o IRC. A maior parte deste não derivam do próprio protocolo, mas dos seus *clientes*, *utilizadores* do IRC e o modo como o fazem. Muitos *clientes* permitem que os *servidores* tenham acesso a mais recursos (ficheiros, programas,...) que seria recomendável. Qualquer utilizador do IRC necessita de tomar bastantes precauções e escolher cuidadosamente o seu programa *cliente*.

O MBONE (Multicast backbone) é a fonte de um novo conjunto de serviços na *Internet*, cuja acção consiste em expandir serviços de conferência em tempo-real, através de serviços baseados em texto, como o *Talk* e o *IRC*, para incluir potencialidades audiovisuais.

Este é um serviço ainda em desenvolvimento, sendo por isso uma preocupação reduzida em termos de segurança. Negações de serviços não intencionais podem ocorrer, pois os dispositivos audiovisuais consomem muita memória.(*Chapman & Zwicky,1995*)

TRADUÇÃO DE NOME

Este é o serviço que permite fazer a tradução dos nomes dos *hosts* , para os endereços numéricos IP. Nos primeiros tempos da *Internet* , era possível a cada *site* manter uma tabela dos *hosts* que listasse o nome e o número de cada máquina da *Internet*, que pudesse vir a ser de interesse . Com milhões de *hosts* ligados, não é pratico manter uma lista de *hosts* e muito menos que todos os *sites* o façam. Por esse motivo, o *Domain Name Service* (DNS) permite que cada *site* mantenha a informação dos seus próprios *hosts* e que seja capaz de encontrar a informação sobre outros *sites*.

O DNS é um serviço para o uso do utilizador final, mas é também um serviço para ser usado por outros serviços, tais como o SMTP, FTP ou o TELNET, permitindo o acesso a *hosts* através dos seus nomes e não pêlos seus endereços IP, o que facilita muito a tarefa dos utilizadores.

O principal risco do uso do DNS é o de se disponibilizar mais informação do que se pretende. Por exemplo, o DNS permite que esteja disponível ao utilizador externo, informação sobre o *software* e *hardware* existentes no sistema. Este tipo de informação é, geralmente, mantida confidencial.(*Chapman & Zwicky,1995*)

SERVIÇO DE GESTÃO DE REDES

Existe uma variedade de serviços usados para gerir e manter redes. Tais serviços não são geralmente usados pelos utilizadores, mas são ferramentas muito importantes para a gestão de redes.

As duas ferramentas mais comuns são o *Ping* e o *Traceroute*. Eles não têm os seus próprios protocolos, mas fazem uso do *Internet Control Message Protocol* (ICMP).

O *Ping* tem como finalidade fazer um teste de alcance. Ele informa se é possível ou não, entregar ou receber um pacote (de dados) de um determinado *host* e quanto tempo levará o referido pacote a alcançar o destino.

Por sua vez, o *Traceroute* verifica, não só, se é possível alcançar um determinado *host*, mas também a trajectória que o referido pacote ira tomar até alcançar o seu destino.

Estas ferramentas são muito úteis para analisar e fazer um levantamento de problemas que possam existir entre dois pontos da rede. Por não existirem *servidores* específicos para estes dois serviços não é possível bloqueá-los. Pode ser feita uma filtragem dè pacotes para prevenir que estes sejam transmitidos ou recebidos no sistema. Estes são outro tipo de serviços que não representam riscos adicionais de segurança. Podem ser usados para realizar ataques de negação de serviços, mas na mesma escala que alguns serviços já vistos.

Simple Network Management Protocol (SNMP) é um protocolo desenhado para tornar mais fácil a gestão centralizada do equipamento de uma rede (*routers, hubs,...*). As estações de gestão podem pedir informação sobre o equipamento da rede em termos de estado e qualidade das comunicações, via SNMP.

O Maior risco em termos de segurança associado a este protocolo, é o de um atacante tomar controle do equipamento da rede e reconfigura-lo para o seu próprio uso.(*Chapman & Zwicky,1995*)

SERVIÇO DE TEMPO

Network Time Protocol (NTP) é um serviço de *Internet* que faz a gestão dos relógios do sistema. A sincronização do tempo entre duas máquinas é importante por diversos motivos. Do ponto de vista de segurança, a análise dos tempos exactos de acessos ao sistema no ficheiro de transacções, pode ajudar a analisar situações de violações do sistema.

A existência de relógios sincronizados é importante para prevenir os chamados ataques *Playback* , em que o atacante grava uma determinada iteração e volta a repeti-la periodicamente em intervalos de tempo regulares. Se forem fixadas marcas de tempo na transacção, o sistema dará uma mensagem de erro, na vez seguinte que se tentar executar.(*Chapman & Zwicky,1995*)

SISTEMAS DE FICHEIROS DE REDE

Existem vários protocolos disponíveis, que permitem aos computadores configurar sistemas de ficheiros que estejam fisicamente conectados à outros computadores. Esta é uma situação desejável, pois permite que os utilizadores tenham à sua disposição ficheiros remotos sem que necessitem de os transferir. Mas por outro lado é um serviço muito perigoso, pois significa que se esta a autorizar que utilizadores remotos leiam documentos do sistema sem que para isso tenham que se identificar, nas maquinas que acedem.

O *Network File System(NFS)* e o *Andrew File System(AFS)* são os mais usados sistemas de ficheiros do *Unix*.

O NFS foi desenhado para uso em redes locais (LAN) e garante rápida capacidade de resposta , grande nível de confiança e sincronização de tempo. Por sua vez, o AFS foi desenhado para funcionar em redes de grandes dimensões e é tolerante à performances mais pobres e níveis mais baixos de confiança.

Existem sérios problemas de segurança relacionados com o NFS. Se este serviço não tiver sido devidamente configurado, um atacante pode simplesmente configurar o NFS no sistema de ficheiros locais. Pelo modo como este serviço funciona, as máquinas *clientes* podem ler e alterar ficheiros armazenados no *servidor* sem terem que directamente aceder a este, ou terem que se autenticar.

Como o NFS não regista as transacções efectuadas pelos utilizadores, torna-se impossível saber se algum utilizador teve acesso aos ficheiros do sistema. Apesar disso, o NFS garante uma forma de se controlar as máquinas que acedem aos ficheiros do sistema e quais os ficheiros que devem estar disponíveis. No entanto, este sistema de ficheiros não é muito seguro para ser usado na *Internet,* pois possui um mecanismo muito fraco de autenticação de utilizadores e um atacante pode conseguir com alguma facilidade permissão de acesso.

Não existem, portanto, muitos ganhos em autorizar o seu uso por utilizadores externos, pois adiciona pouca funcionalidade e cria um grande problema de segurança.(*Chapman & Zwicky, 1995*).

CAPÍTULO II

PROTECÇÃO DO SISTEMA

Para se desenhar um esquema de protecção eficiente, é necessário conhecer-se as técnicas de protecção mais modernas actualmente existentes e a sua forma de implementação. O presente capítulo faz uma abordagem a tais técnicas. Estes conhecimentos são posteriormente aplicados na elaboração da proposta da política de segurança.

Não existe nenhum modelo que possa resolver todos os problemas de segurança com que se deparam os sistemas. Por exemplo, nenhum modelo pode impedir um utilizador hostil, tendo permissões de acesso, de intencionalmente destruir informação ou retirar informação do sistema. Pode ser montado um sistema que proteja eficientemente contra acidentes, utilizadores pouco habilitados ou contra actos externos maliciosos, mas não se pode proteger contra legítimos usuários sem destruir as suas permissões de acesso ao sistema.

Nenhum modelo de segurança garante "protecção total". Pode-se conseguir que as violações aos sistemas sejam diminutas. Mesmo os mais seguros sistemas existentes, devem esperar que a qualquer momento possa acontecer um acidente de segurança. A protecção montada para o sistema pode garantir, nestas situações, que tais acidentes não provoquem danos irreparáveis

ESTRATÉGIAS DE PROTECÇÃO DE DADOS

A adopção de uma das estratégias seguintes irá garantir maior protecção dos sistemas:

- encriptação. Se o atacante conseguir aceder aos dados, não poderá fazer qualquer uso dos mesmos, nem mesmo fazer alterações, sem o conhecimento do algoritmo de encriptação;

- uso de um *firewall* para isolar a rede interna do mundo exterior;

- isolar a rede local do mundo exterior;

- criar uma segunda rede interna para a informação mais confidencial;

- desactivar todos os serviços que não sejam indispensáveis ao funcionamento do sistema. Garantir a existência de mecanismos que restrinjam a conectividade à rede.

2.1 PROTECÇÃO DO HOST

Este é, sem dúvida, o mais comum modelo de segurança implementado pelos gestores de redes e consiste, basicamente, no reforço da segurança de cada máquina *host* em separado. O problema com este tipo de segurança surge quando se tem que lidar com um grande número de máquinas na rede.

A maior contrariedade a uma efectiva segurança através do *host* nos ambientes modernos de computação é a complexidade e diversidade dos mesmos, pois em muitos casos as organizações têm máquinas de diferentes fabricantes, muitas vezes com sistemas operativos diferentes e cada um deles com os seus problemas específicos de segurança.

Mesmo nos casos em que as máquinas são todas do mesmo fabricante, diferentes versões do mesmo sistema operativo podem originar problemas.

No caso em que as máquinas são do mesmo fabricante e está instalada a mesma versão do sistema operativo em todas as máquinas, se existirem diferentes tipos de configurações, podem surgir problemas de segurança.
É importante a uniformização, sempre que possível, do *hardware*, *software* e configurações usadas numa rede.

Existe também o perigo dos utilizadores com privilégios de acesso às máquinas. Com o aumento do número de máquinas numa rede, aumenta do mesmo modo o número de utilizadores autorizados. Garantir a segurança do *host* torna-se deste modo cada vez mais difícil, pois não é possível assegurar que estes novos utilizadores não possam cometer falhas que coloquem em perigo a segurança de cada *host*.

A segurança do *host* é mais apropriada para pequenos *sites* da *internet*. Garantir a segurança do *host* implica um grande investimento de tempo, trabalho e dinheiro. O acesso aos recursos da rede deve ser restrito e os utilizadores autorizados devem apenas ter os privilégios que necessitam para realizar as suas actividades.

2.2 PROTECÇÃO DA REDE

Com o crescimento das redes informáticas, a segurança do *host* vai-se tornando cada vez mais difícil de implementar. A segurança da rede emerge, então, como a solução mais viável.

O modelo de segurança de rede permite que se concentrem atenções no controle dos acessos à rede, no lugar de se tentar garantir a segurança *host* a *host*. Este tipo de abordagem inclui a construção de *firewalls* para a protecção do sistema de *internet* e redes e o uso da criptografia para proteger os dados em trânsito na rede.

Uma rede informática pode ser muito consistente usando o modelo de segurança de rede. Um único *firewall* consegue proteger centenas de computadores contra ataques externos, independentemente do nível de segurança de cada uma das máquinas.

2.2.1 FIREWALLS

O termo *Firewall* é inspirado da construção civil, onde esta palavra é empregue nos casos em que se pretende implementar um dispositivo que sirva para impedir a propagação do fogo num edifício, em caso de incêndio. Um *firewall* é geralmente instalado no ponto da rede onde se conecta a rede à *Internet* .Tem como objectivo prevenir que os perigos da *Internet* se propaguem pela rede. Ele serve para alguns fins, a saber:

- Restringir as entradas e saídas da rede a um único ponto, cuidadosamente controlado.

- Evitar que os atacantes se "aproximem" das outras defesas da rede.

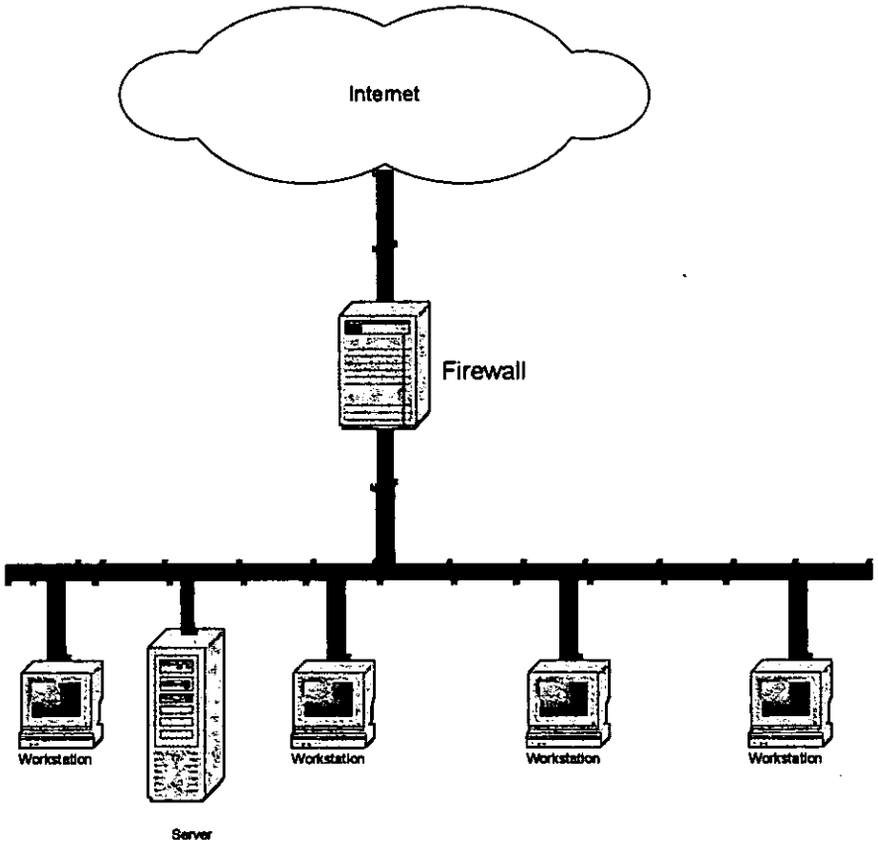


Fig. 1. Rede Com ligação à *Internet* protegida por um *Firewall.(Chapman & Zwicky,1995)*

Todo o tráfego vindo ou saído da *Internet* , passa pelo *firewall*. Por este motivo, este tem a possibilidade de verificar se o referido tráfego é aceitável em termos das políticas de segurança da instituição. Aceitável significa que todos os serviços respeitam as regras de segurança do sistema.

Em termos lógicos, um *firewall* é um separador, um elemento restritivo , um analisador. A sua implementação física é geralmente um conjunto de componentes de *hardware* – Um *router,* computador *host,* ou uma combinação de *routers* , computadores e uma rede com *software* apropriado. A maneira como este equipamento deve ser configurado, irá depender da política de segurança adoptada pela organização e do orçamento disponível para a sua implementação.

Um *firewall* geralmente nunca consiste num único objecto existindo, no entanto, a tendência para, nos tempos mais recentes, os grandes fabricantes de produtos de segurança concentrarem numa única máquina todos os elementos de segurança. Os diversos componentes de um *firewall* que não esteja concentrada numa única máquina, realizam outras actividades para além de desempenharem tarefas de segurança.

2.2.1.1 TIPOS DE FIREWALLS

Os *firewalls* dividem-se em duas categorias básicas (*Chapman & Zwicky,1995*):

FIREWALL DE NÍVEL DE REDE

Estes são geralmente *routers* com uma poderosa capacidade de filtragem de pacotes. Utilizando um *firewall* de nível de rede , pode-se conceder ou recusar o acesso à uma rede.

Este tipo de *firewall* tem diversos tipos de deficiências. Muitos *routers* são vulneráveis a ataques do tipo *spoofing e,* por outro lado, o seu desempenho fica muito afectado quando são implementados procedimentos de filtragem muito rigorosos.

FIREWALL DE APLICATIVO PROXY

Neste tipo de *firewall* , o *Gateway* faz a gestão das conexões entre a rede interna e utilizadores remotos. Neste caso os pacotes *IP* não são entregues directamente à rede interna. Em vez disso, um tipo de tradução ocorre, com o *Gateway* a funcionar como canal e como intérprete. O aplicativo *proxy* deve ser configurado para cada serviço de rede, incluindo FTP, *Telnet,* HTTP e correio.

2.2.1.2 A ACÇÃO DO FIREWALL

FIREWALL É O CENTRO DAS DECISÕES DE SEGURANÇA.

O *firewall* deve ser sempre visto como um ponto de controlo. Todo o tráfego de entrada ou de saída deve passar por ele. Ele permite que as atenções sejam concentradas num único ponto, o ponto onde são verificados todos os elementos de segurança.

Focando a segurança num único ponto, torna-se muito mais eficiente a protecção, que separando as decisões e tecnologia pela rede, tentando cobrir as várias regiões desta.

FIREWALL PODE REFORÇAR AS POLITICAS DE SEGURANÇA

O *firewall* reforça as políticas de segurança, ao permitir que apenas os serviços autorizados sejam executados, desde que eles próprios cumpram as regras estabelecidas para o efeito.

FIREWALL PODE CONECTAR A ACTIVIDADE DA INTERNET DE MODO EFICIENTE

Porque todo o tráfego da rede passa pelo *firewall,* este possibilita que se faça uma recolha de informação sobre o modo como a rede e o sistema estão a ser usados. Havendo um único ponto de acesso à rede, o *firewall* pode registar tudo o que ocorre entre a rede e o mundo exterior.

O FIREWALL LIMITA A EXPOSIÇÃO DA REDE

Algumas vezes o *firewall* poderá ser usado para separar um sector da rede dos restantes. Com isto consegue-se evitar que problemas que afectam uma determinada área, se propaguem pela rede.

Outra situação ocorre quando existe um sector da rede que seja mais confiavel (em termos do seu desempenho) que os restantes, ou que seja mais sensível (em termos de informação armazenada). Em qualquer um dos casos, a existência do *firewall* pode impedir que um problema na rede se propague.

2.2.1.3 LIMITAÇÕES DO FIREWALL

Os *firewalls* garantem uma grande protecção contra ataques vindos do exterior mas não são uma solução completa de segurança. Existem problemas que não podem ser resolvidos por este e que devem ser combatidos incorporando de forma complementar a segurança fisica, segurança de *host* e a educação dos utilizadores em todo o plano de segurança.

O FIREWALL NÃO PROTEGE CONTRA:

UTILIZADORES INTERNOS MAL INTENCIONADOS

Um *firewall* pode impedir que um utilizador envie informação valiosa para fora da rede, inibindo a ligação com o exterior. Mas este mesmo usuário pode copiar a informação para uma *disket*, banda magnética ou papel e transporta-la para fora da rede.

Se o atacante vier de dentro da organização, o *firewall* nada pode fazer para impedir a sua acção. Os Utilizadores internos podem "roubar" dados, destruir *hardware* ou *software* sem terem que passar pelo *firewall*.

CONEXÕES QUE NÃO PASSEM POR ELE

Um *firewall* pode controlar efectivamente o tráfego que passe por si mas, por outro lado, nada pode fazer ao tráfego que não passe. Muitas vezes os peritos técnicos ou administradores da rede constroem as suas próprias portas alternativas de entrada e saída da rede, por não pretenderem que as restrições determinadas nas políticas de segurança os abranjam, também. Nestes casos o *firewall* nada pode fazer, pois trata-se de um problema de gestão e não de um problema técnico.

FORMAS DE ATAQUES DESCONHECIDAS.

Um *firewall* é desenhado para proteger contra formas de ataques conhecidas. Por esse motivo, este não pode, automaticamente, proteger contra todas as novas formas de ataques que surgem. Periodicamente surgem novas formas de se executarem ataques a sistemas informáticos. Não se pode conseguir que um *firewall* se mantenha eternamente actualizado e com eficácia máxima.

O FIREWALL NÃO PROTEGE CONTRA VÍRUS

Um *firewall* não consegue impedir a entrada de *vírus* na rede. Apesar de muitos *firewalls* fazerem um *scann* à todo o tráfego de entrada para determinar se o mesmo pode ou não passar pela rede, este *scann* não visa o conteúdo dos dados, mas sim os endereços de origem e de destino. Mesmo usando um pacote de filtragem sofisticado, a protecção contra um *vírus* num *firewall* não é muito prática, pois existem diversas formas de *vírus* que se podem esconder nos dados.

Detectar um *vírus* num pacote aleatório de dados, passando por um *firewall* é bastante difícil e requer que este:

- verifique se o pacote é parte de um programa;

- determine a forma que o programa deveria ter;

- determine se eventuais mudanças podem ter sido causadas por *vírus*.

A forma mais eficiente de protecção contra *vírus* é a través da instalação de um *software*(Anti-vírus) no *host* e a educação dos usuários no que respeita aos perigos que estes representam e as precauções a tomar.

2.3 PROTECÇÃO DA INFORMAÇÃO EM TRÂNSITO

A informação em trânsito na *Internet* corre sempre o risco de ser interceptada. Actos de espionagem comercial ou simples curiosidade levam a que *crackers* tentem conhecer o conteúdo de mensagens em trânsito. Existe também o risco de ocorrer um *ataque de navegação de serviços*.

A intercepção de mensagens em trânsito tem sido evitada graças ao recurso à criptografia.

2.3.1 CRIPTOGRAFIA

A Criptografia é a técnica actualmente utilizada, com grande eficiência, para a protecção da informação em trânsito na *Internet*. É um conjunto de técnicas usadas para manter a informação segura.

Criptografar significa transformar uma mensagem em uma segunda mensagem , usando uma função e uma chave criptográfica especial (Garfinkel & Spafford,1999)

Os sistemas modernos de criptografia consistem de dois processos complementares :

- criptografia: processo pelo qual uma mensagem (texto original) é transformada em uma segunda mensagem (texto cifrado), usando uma função (algoritmo de criptografia) e uma chave criptográfica especial;

- decifragem: processo inverso, pelo qual o texto cifrado é transformado no texto limpo, usando-se uma segunda função complexa e uma chave de decifragem. Em alguns sistemas, a chave criptográfica e a chave de cifragem são iguais, mas em outros não.

O objectivo da criptografia é tornar difícil a reprodução de um texto a partir de outro(cifrado), sem o conhecimento da chave e algoritmo correspondentes. Além disso, dificultar ao máximo a chance de que se descubra qual a chave que tornaria isso possível.

Apesar de inicialmente ter sido largamente utilizada na área militar, a criptografia tornou-se uma ferramenta usada nos negócios e no comércio, passando a ser uma tecnologia de uso dual, com aplicações civis e militares.

Para o utilizador a criptografia é uma maneira de comprar certezas e reduzir riscos em um mundo incerto. *(Garfinkel & Spafford,1999)*

A criptografia pode ser usada com os seguintes objectivos:

- proteger a informação armazenada no sistema contra acessos não autorizados;

- proteger a informação em trânsito no sistema;

- detectar alterações acidentais ou intencionais dos dados do sistema;

- verificar se o autor de um determinado documento é, de facto, quem reclama ser.

2.3.1.1 SISTEMAS CRIPTOGRÁFICOS

Os sistemas criptográficos actualmente em uso podem ser divididos em duas categorias:

A primeira é a dos programas e protocolos usados para a criptografia de mensagens de correio electrónico. Estes programas encriptam as mensagens e enviam-nas pela *Internet* ou armazenam-nas. Podem também ser usados para criptografar arquivos armazenados em computadores, dando-lhes uma protecção adicional.

A segunda é a de protocolos de rede usados para oferecer confidencialidade, autenticação e não-repúdio em ambientes de rede. Tais sistemas exigem interacção em tempo real entre *clientes* e *servidores* , de modo a que estes funcionem devidamente.

2.3.1.2 OS ELEMENTOS DA ENCRIPTAÇÃO/DECRETAÇÃO

Existem várias formas de se usar um computador para *encriptar* ou *decriptar* informação. Em todo o caso, todos os chamados *sistemas de encriptação* possuem alguns elementos comuns, a saber:

Algoritmo de Encriptação

Este algoritmo é a função, algumas vezes com alguma fundamentação matemática, que realiza a tarefa de *encriptar* ou *decriptar* os dados.

Chave de Encriptação

Esta é usada pelo algoritmo de encriptação para determinar o modo como os dados são *encriptados* ou *decriptados.* Quando uma porção de informação é *encriptada*, é necessário indicar a *chave* correcta para se poder aceder à informação original.

Comprimento da Chave

As *chaves de encriptação* têm sempre um comprimento, que é um factor determinante para manter a informação secreta. Quanto mais longa for a *chave*, mais difícil se torna desvenda-la. O tamanho mínimo recomendável depende do algoritmo usado.

Texto Original

A informação que se pretende *encriptar.*

Texto Encriptado

A informação *encriptada.*

2.3.1.3 ATAQUES A ALGORITMOS DE CRIPTOGRAFIA

Para se usar a criptografia com o objectivo de se proteger a informação, é necessário ter em mente que pessoas não autorizadas podem tentar decifrá-la. Deste modo, os sistemas de segurança deverão ser resistentes aos ataques directos. Vejamos alguns tipos de ataques mais comuns à informação transmitida na *Internet:*

a) Ataque de Busca de Chave:

A maneira mais simples de quebrar um código, é testar todas as chaves possíveis, até que se descubra a chave correcta, desde que se possa reconhecer os resultados do uso da chave certa. A maioria das tentativas será malograda, mas uma delas terá sucesso e permitirá entrar no sistema ou decifrar a mensagem. Não existe uma maneira de se defender contra este tipo de ataque, pois não é possível evitar que um atacante tente decifrar as mensagens com todas as chaves possíveis. Mas, este tipo de ataque não é eficiente e muitas vezes nem é possível.

Tomando como exemplo o algoritmo *RC4,* usado comumente em navegadores para criptografar informação enviada na *Word Wide Web.* Este algoritmo pode ser usado com qualquer tamanho de chave entre 1 e 2048 *bits.* Mas geralmente é usado com uma chave secreta de 40 *bits* ou uma de 128 *bits.* Com uma chave de 40 *bits*, há 2^{40} chaves possíveis de testar. Mesmo um computador super potente , que possa testar um milhão de chaves por segundo, levaria 13 dias a testar todas as hipóteses possíveis.

b) Análise de Criptografia:

Se o tamanho fosse o único factor determinante da segurança de um código, bastaria usar chaves de 128 *bits* (muito mais seguras que as de 40) para transmitir informação com segurança. Muito raramente é usado um ataque de busca de chave para revelar o conteúdo de uma mensagem criptografada. Em vez disso, a maioria dos algoritmos pode ser quebrado, usando uma combinação de matemática sofisticada e um bom poder de computação. Como resultado, muitas mensagens podem ser quebradas sem o conhecimento da chave. Um analista de criptografia habilidoso, pode decifrar um texto cifrado sem conhecer sequer o algoritmo de criptografia. Um ataque de análise de criptografia pode ter dois objectivos possíveis:

- O analista de criptografia pode ter o texto criptografado e querer ter o original.

- O analista pode ter o texto criptografado e querer descobrir o algoritmo usado para criptografa-lo.

Alguns ataques de *analise de Criptografia* aplicados ao trafico na *WWW(Garfinkel e Spafford,1999)*:

c) Ataque de Texto Conhecido

Neste tipo de ataque, o analista de criptografia dispõe de um bloco de texto original e de um bloco correspondente do criptografado. Embora possa parecer difícil de acontecer, na verdade é bem comum, quando a criptografia é usada para proteger correio electrónico (com parágrafos padrão no inicio de cada mensagem) ou discos duros (com estruturas conhecida sem locais predeterminados do disco) O objectivo do ataque do texto conhecido é determinar a chave criptográfica (e possivelmente o algoritmo) que pode então ser usado para decifrar outras mensagens.

d) Ataque ao Texto Escolhido

Neste tipo de ataque, o analista de criptografia pode criptografar blocos de dados escolhidos a partir do alvo do ataque, criando um resultado que ele pode então analisar. Este tipo de ataque é mais simples do que pode parecer. Por exemplo, o alvo do ataque pode ser um vínculo de rádio que criptografa e retransmite mensagens recebidas por telefone. O objectivo de um ataque a um texto escolhido, é a determinação de uma chave criptográfica, que pode ser usada para decifrar outras mensagens.

e) Análise Diferencial de Falha

Este ataque funciona contra sistemas criptográficos em *hardware*. O mecanismo está sujeito a factores ambientais (calor, radiação, fadiga) de forma a induzir a falhas durante a operação de

criptografia ou decifragem. Estas falhas podem ser analisadas e, a partir delas, pode-se entender o estado interno do mecanismo, incluindo a chave ou o algoritmo criptográfico.

A forma mais eficiente de avaliar a qualidade de um algoritmo é publica-lo e esperar que alguém descubra uma vulnerabilidade. Este processo de revisão entre pares não é perfeito, mas é melhor que não realizar revisão alguma. A verdadeira segurança criptográfica reside na abertura e na revisão dos pares.

f) Ataques de Geração

Estes ataques são os mais populares, por serem os mais simples de serem compreendidos. Estes ataques tentam inferir a chave secreta com base na chave pública correspondente. No caso do sistema *RSA,* o ataque pode ser feito gerando um número associado à chave pública. Com outros tipos de sistemas, o ataque exige a resolução de outro tipo de problemas matemáticos.

Hoje em dia, o poder do *RSA* depende da faculdade de gerar grandes números. Há alguns métodos eficientes para gerar pequenas classes de números com certas propriedades, mas o problema global da geração é ainda considerado difícil do ponto de vista computacional.

g) Ataques Algorítmicos

Outra forma de atacar um sistema criptográfico de chave pública seria descobrir uma falha fundamental no problema matemático no qual se baseia o referido sistema.

2.3.1.4 PODER CRIPTOGRÁFICO

Formas diferentes de criptografia quase nunca são iguais. Alguns sistemas não protegem bem os dados, permitindo que a informação criptografada seja decifrada sem o conhecimento da chave. Outros são resistentes aos ataques mais determinados.

A capacidade de um sistema criptográfico proteger informação é chamada poder (Garfinkel & Spafford,1999)

O poder depende de muitos factores , a saber:

- Grau de segredo da chave.

- A dificuldade de descobrir a chave certa através de tentativas (busca da chave). As chaves mais longas, são também as mais difíceis de serem descobertas.

- A dificuldade de inverter o algoritmo de criptografia, sem conhecer a chave criptográfica (quebra do algoritmo criptográfico).

- A existência de "buracos" ou caminhos pêlos quais um arquivo criptografado pode ser decifrado, sem o conhecimento da chave.

- A capacidade de decifrar toda uma mensagem criptografada, se a decifragem de uma parte dela for conhecida. Este é chamado ataque do texto conhecido.

- As propriedades do texto original e o conhecimento delas por um atacante. Por ex. se as mensagens de um sistema começam e acabam sempre com um texto conhecido.

2.3.1.5 LIMITAÇÕES DA CRIPTOGRAFIA

A criptografia tem também as suas limitações. Em algumas situações esta nada pode fazer:

A Criptografia não pode proteger documentos não encriptados

Mesmo que o servidor *Web* esteja configurado para enviar apenas arquivos *encriptados* , os originais (não encriptados) ainda se mantêm no *servidor* . Quem invadir o sistema, terá sempre acesso aos dados.

A Criptografia não protege contra chaves criptográficas roubadas

Um dos objectivos da criptografia passa por tornar possível às pessoas que possuem as *chaves criptográficas* , decifrar mensagens e arquivos. Por este motivo, qualquer atacante que consiga roubar estas chaves pode decifrar os arquivos ou mensagens.

A Criptografia não pode proteger contra ataques ao serviço

Protocolos criptográficos como o SSL são bons para proteger informação. Mas, como já foi dito, um atacante nem sempre tem como objectivo aceder à informação. Em instituições como bancos, um atacante pode causar muitos danos e prejuízos se conseguir , por exemplo, interromper as comunicações.

A Criptografia não pode proteger de um programa de criptografia sabotado

Os programas de criptografia podem ser alterados, tornando-os inúteis. O mais conhecido destes ataques é aquele realizado sobre o *Netscape Navigator* de modo a que este use sempre a mesma chave criptográfica.

Teoricamente, não existe possibilidade de eliminar as chances deste tipo de ataque ocorrer. Existe sempre o risco, quer a criptografia seja usada, ou não. No entanto, tais riscos podem ser

minimizados, obtendo os programas de criptografia por meio de canais próprios. Podem também ser usadas assinaturas digitais e técnicas como assinaturas em código, para detectar alterações aos programas criptográficos.

A criptografia não pode proteger de erros ou utilizadores internos mal intencionados

Os seres humanos são o elo mais fraco num sistema. A criptografia não pode proteger contra erros (ou acções intencionais) que os utilizadores autorizados possam cometer e que ponham a descoberto os mecanismos de protecção.

Embora a criptografia seja um elemento importante de segurança na *Web*, não é o único. Esta não pode garantir a segurança do sistema se as pessoas puderem invadi-lo de outra forma. Mas a criptografia protege os dados, o que ajuda a minimizar o impacto de uma invasão.

CAPITULO III

POLÍTICAS DE SEGURANÇA

A segurança numa rede consiste em uma série de soluções técnicas para problemas não técnicos. Por muitos recursos que se despendam, nunca se está completamente livre da necessidade de resolver problemas de perda acidental de dados ou destruição intencional dos mesmos. Por diversos motivos, tais como deficiência do *software*(bugs), acidentes, erro humano ou ataque de um *hacker*, qualquer sistema pode ficar seriamente afectado.

É tarefa do profissional responsável pela segurança do sistema, ajudar os gestores da organização a decidir quanto tempo e dinheiro se deve dispender na protecção da informação. Consiste também das suas tarefas, garantir que a organização tenha políticas, linhas de orientação e procedimentos que garantam uma boa aplicação dos recursos disponíveis. Finalmente, o profissional deve fazer auditoria ao sistema para garantir que os mecanismos de controlo estejam devidamente implementados, de tal modo que as políticas de segurança sejam respeitadas.

O presente capítulo aborda o modo de se deve elaborar uma política de segurança, os principais aspectos a tomar em consideração e as possíveis linhas de orientação a adoptar.

Existem dois princípios muito importantes no planeamento da segurança de um sistema:

- As políticas e estratégias devem ser conduzidas do topo para a base (em termos hierárquicos) na organização. As figuras de topo devem encarar a segurança como um factor extremamente importante, definindo regras que deverão ser seguidas de igual modo por todos os utilizadores.

- A segurança efectiva do sistema significa proteger informação. Todo o planeamento, políticas e procedimentos devem sempre reflectir a necessidade de proteger a informação.

3.1 ESTRATÉGIAS DE SEGURANÇA

MÍNIMOS PRIVILÉGIOS

Este talvez seja o princípio mais fundamental de segurança (num contexto mais amplo, não apenas em termos informáticos). Aqui, qualquer objecto (utilizador, administrador de rede, programas...) terá apenas os privilégios mínimos necessários para realizar as suas tarefas. Mínimos privilégios é um importante princípio para limitar a exposição da rede à ataques e minimizar os danos causados por algum ataque bem sucedido.

O utilizadores não necessitam de ter acesso à todos os serviços de *Internet*. Não necessitam de ter permissão para ler ou escrever em todos os ficheiros do sistema. Não necessitam de conhecer a *password* do sistema. Estas são algumas das restrições que podem ser aplicadas.

A teoria dos mínimos privilégios sugere que se deve explorar formas de reduzir os privilégios dos utilizadores ao mínimo possível.

Existe um problema que geralmente ocorre ao se implementar esta estratégia de segurança:

- A ânsia de querer limitar os privilégios, pode muitas vezes levar a que se concedam menos privilégios que o mínimo necessário para os utilizadores realizarem as suas tarefas.

FALHA EM SEGURANÇA

Outro princípio fundamental de segurança é o da *falha em segurança.* Isto significa que se um sistema tiver uma falha, é essencial que esta ocorra de tal modo que, mesmo assim, o sistema consiga impedir que o atacante entre no sistema. Legítimos utilizadores ficarão impossibilitados de aceder ao sistema, até que este esteja recuperado. Nenhum serviço será autorizado, nem mesmo à utilizadores com permissões. Desta forma é garantido que não haverão ataques através deste sistema. Por exemplo, se um *router* de filtragem de pacotes falhar, nenhum pacote deve circular pela rede, seja qual for a sua proveniência

LIGAÇÃO MAIS FRACA

Uma rede é tanto mais segura, quanto o seu ponto mais fraco também o for. (Chapman and Zwicky,1995)

Este é um princípio fundamental da segurança de uma rede. Os atacantes procuram sempre os pontos mais fracos da rede, daí que estes devem merecer uma atenção especial. Devem ser tomadas medidas para eliminar esses pontos fracos, ou então monitorar aqueles que não poderem ser eliminados.

Haverá sempre uma ligação mais fraca em qualquer rede, mas a estratégia deve consistir em tornar esta ligação suficientemente forte, de tal modo que a sua força seja proporcional aos riscos.

PONTO DE ESTRANGULAMENTO

Esta estratégia força qualquer utilizador externo a usar um canal estreito, devidamente controlado e monitorado. Neste contexto, o *firewall* funciona como o canal estreito. Quem tentar realizar um ataque à rede, vai ter que passar pelo *firewall*. O *ponto de estrangulamento* não terá utilidade se existirem formas alternativas de acesso à rede. Se as atenções dos gestores da rede estiverem dispersas, mais facilmente o atacante poderá violar o sistema.

A maior aplicação deste princípio na segurança da rede está na escolha da posição a tomar pelos gestores do sistema em relação à segurança. Existem duas alternativas possíveis:

- *proibição por defeito:* são especificados os serviços autorizados, ficando proibidos todos os restantes;
- *autorização por defeito:* são especificados os serviços proibidos, ficando autorizados todos os restantes.

PROIBIÇÃO POR DEFEITO

O QUE NÃO ESTIVER EXPRESSAMENTE AUTORIZADO, ESTA PROIBIDO

É o reconhecimento de que tudo o que seja desconhecido para o sistema pode representar perigo. Com a proibição por defeito são proibidos todos os serviços e ao se determinar os autorizados, deve ser feito:

- um exame dos serviços que os utilizadores pretendem;
- uma análise das suas implicações em termos de segurança;
- autorização apenas dos serviços conhecidos, depois de garantir que os mesmos são imprescindíveis aos utilizadores.

Os serviços devem ser disponibilizados após uma análise caso a caso, começando por contrabalançar as implicações de segurança de cada um, com a necessidade que os utilizadores têm dos mesmos.

AUTORIZAÇÃO POR DEFEITO

O QUE NÃO ESTIVER EXPRESSAMENTE PROIBIDO, ESTÁ AUTORIZADO.

Geralmente, os utilizadores preferem que seja usada esta estratégia, assumindo que os serviços deverão estar sempre disponíveis e que os potencialmente perigosos serão posteriormente proibidos. Mas esta não é uma boa estratégia, pois pressupõe que são conhecidos todos os riscos que podem advir do exterior, o que é quase impossível. Quando não se sabe se um serviço representa perigo, este não vai constar da lista de proibições. Neste caso, será autorizado até que uma situação grave aconteça. As consequências poderão ser irreparáveis.

Por outro lado, esta estratégia tende a degenerar numa "guerra" entre os gestores do sistema e os utilizadores da rede, uma vez que os gestores têm que preparar constantemente acções de defesa contra a acção (ou inacção) dos utilizadores, enquanto estes procuram sempre descobrir novas formas de contornar as limitações impostas pelos gestores. Inevitavelmente existirão períodos de vulnerabilidade do sistema, no intervalo de tempo entre a inicialização do sistema, a descoberta do problema e o tempo em que este é resolvido.

A decisão sobre qual a melhor opção depende muito do ponto de vista de quem toma posição sobre o assunto. Do ponto de vista dos administradores do sistema, a decisão mais correcta seria a *proibição por defeito*, enquanto que para os utilizadores a melhor opção seria a *autorização por defeito.*

PARTICIPAÇÃO UNIVERSAL

De modo a obterem uma segurança efectiva, os gestores de sistemas tendem a adoptar estratégia de participação universal. Se algum utilizador for capaz de contornar o sistema de segurança montado, então qualquer atacante pode também fazer, atacando em primeira instância este mesmo utilizador. Por exemplo, a utilização de *modems* pode servir como alternativa à passagem pelo *firewall,* abrindo uma "porta" à passagem do *hackers.*

Podem existir tentativas de violar as normas estabelecidas no sistema. É necessário que os utilizadores estejam alertas e reportem todo comportamento estranho que julguem relacionado com segurança.

A participação dos utilizadores pode ser voluntária, quando estes são sensibilizados para a necessidade de participarem de forma construtiva na garantia da segurança do sistema. Pode ser compulsiva, quando os utilizadores são obrigados a cumprir certas normas determinadas pelos gestores da rede, ou pode também ser uma combinação destas duas hipóteses.

A participação voluntária é a mais aconselhável, pois ela exige que os utilizadores estejam conscientes dos riscos que existem e da importância da sua colaboração.

DIVERSIDADE DE DEFESA

Do mesmo modo que se consegue um reforço na capacidade de segurança da rede pelo uso de um certo número de sistemas diferentes, de forma a obter mais consistência, pode-se também reforçar a segurança através do uso de um certo número de sistemas de tipos diferentes. Se os sistemas de segurança de uma rede forem semelhantes, qualquer atacante que consiga quebrar um deles, conseguirá fazer o mesmo em todos.

A ideia subjacente a diversidade de defesa é a de que usando sistemas de segurança de diferentes características se reduz a possibilidade de ocorrência de uma falha ou erro de configuração que possa comprometer todos os sistemas. Contudo, existem muitas desvantagens deste sistema, em termos de complexidade e custos. A instalação de múltiplos sistemas é sempre mais difícil, morosa e cara, do que a instalação de um único sistema.

3.2 NECESSIDADE DE SEGURANÇA

Um computador é seguro se ele se comportar de maneira esperada (Garfinkel e Spafford,1999).

A elaboração de uma política de segurança visa garantir :

CONFIDENCIALIDADE

Impedir que a informação existente no sistema seja lida ou copiada por alguém que não tenha sido explicitamente autorizado a tal. Isto inclui não apenas a protecção da informação como um todo, mas a protecção da informação em fracções que podem aparentemente não ser importantes, mas que podem ser usados para obter outro tipo de informação confidencial.

INTEGRIDADE DOS DADOS

Proteger a informação, evitando que esta seja apagada ou alterada sem a autorização do proprietário.

DISPONIBILIDADE

Garantir que o sistema esteja sempre disponível, quando dele se necessite. A não disponibilidade do sistema quando os utilizadores autorizados dele necessitem, pode ser tão grave quanto eliminar informação necessária.

CONSISTÊNCIA

Garantir que o sistema se comporta como esperado pelos utilizadores autorizados. Se, repentinamente, o sistema começar a comportar-se de modo radicalmente diferente do que geralmente faz, pode ocorrer um desastre.

CONTROLE

Regular os acessos ao sistema. O acesso ao sistema por parte de utilizadores não autorizados, pode causar sérios problemas. É necessário verificar cuidadosamente quem acede ao sistema e que tipo de actividade vai realizar enquanto estiver no sistema.

AUDITORIA

Os utilizadores autorizados, por vezes também cometem erros ou realizam acções maliciosas. Nestes casos é necessário determinar o que foi feito, por quem e com que consequências. A única maneira de conseguir estes propósitos é tendo registos incorruptíveis de todas as actividades no sistema, que identifiquem inequivocamente os autores e as acções por si realizadas.

Sendo todos estes factores relativos à segurança importantes, o grau de importância dos mesmos varia consoante o tipo de organização referida. No ambiente bancário, a integridade e a auditoria são os factores mais importantes, ocupando um segundo plano a confidencialidade e a disponibilidade. Enquanto, por exemplo, no ambiente académico, a integridade e disponibilidade são os mais importantes.

3.3 RISCOS

O primeiro passo para desenhar uma política de segurança do sistema consiste em responder a três questões básicas:

- o que se pretende proteger?
- contra quem proteger?
- quanto tempo, esforço, recursos e dinheiro se deve despender para obter adequada protecção?

Estas questões constituem a base do processo de avaliação de risco. Esta é uma parte importante de todo o processo de implementação de sistema de segurança, pois não se pode proteger sem conhecer os riscos que se correm e a proveniência dos mesmos. Só então se podem desenhar as políticas e técnicas que devem ser implementadas para reduzir tais riscos.

Os três principais passos a seguir neste processo , são:

1. Identificação dos recursos.
2. Identificação dos riscos.
3. Avaliação de riscos.

Existem várias formas de abordar o processo de avaliação de riscos. O método escolhido para este trabalho e que servirá de base para a elaboração da política de segurança do BCI é o chamado

IN-HOUSE WORKSHOPS , que consiste em reunir e auscultar utilizadores, gestores da rede e executivos da empresa.

3.3.1 IDENTIFICAÇÃO DE RECURSOS

Primeiro deve ser construída uma lista dos *itens* que se pretendem proteger. Esta lista será constituída com base no plano de acções da organização e no senso comum dos gestores da rede. É necessário construir uma lista dos *itens* tangíveis e não tangíveis, lista esta que deve incluir todos os objectos considerados de valor.

Para determinar o valor dos objectos deve-se analisar as consequências que a sua perda causariam ao sistema, ou o custo da sua substituição.

ITENS TANGÍVEIS

- Computadores
- Dados
- Seguranças do Sistema
- Meios de distribuição de *Software*
- Equipamento de comunicação
- Registos de auditoria

ITENS NÃO TANGÍVEIS

- Reputação da instituição
- Confiança dos clientes
- Privacidade dos usuários

3.3.2 IDENTIFICAÇÃO DE RISCOS

Os riscos que podem estar associados ao funcionamento do sistema devem ser listados o mais exaustivamente possível:

- Ataques de *Crackers*
- Introdução de *vírus*
- Empregados maliciosos
- *Bugs* em programas
- Falhas dos equipamentos de comunicação
- Falhas no fornecimento de energia eléctrica

3.3.3 AVALIAÇÃO DOS RISCOS

Após a identificação das situações que podem colocar em risco o normal funcionamento do sistema, é necessário efectuar uma análise aos mesmos.

Em primeiro lugar deve-se analisar a frequência da ocorrência de tais situações. Se o evento ocorrer regularmente, a estimativa pode ser feita com base em registos de tais ocorrências, ou obtendo esta informação através de outras entidades (tais como companhias de electricidade ou de telefones) que possam estar mais capacitadas.

3.4 ANÁLISE DE CUSTOS – BENEFÍCIOS

Depois de terem sido identificados os recursos do sistema e uma vez conhecida a importância de cada um, é necessário determinar os custos que a perda de cada um deles podem implicar, bem como os custos de os proteger e os seus benefícios.

3.4.1 O CUSTO DE PERCA

Esta não é uma tarefa simples. Vários factores (muitas vezes subjectivos) devem ser tomados em consideração quando se faz este tipo de avaliação. Desde o custo de substituição de um determinado *item* da rede, de se ter equipamento fora de serviço, de realizar acções adicionais de treinamento de pessoal, até ao custo de ter a reputação da organização afectada.

Geralmente a atribuição de um valor numérico a esta avaliação, não obedece a critérios rígidos. Por exemplo o custo de perca (definitiva) de equipamento informático pode ser determinado pelo valor monetário ou tempo necessário a dispender para a sua substituição. Deste modo podem ser definidos escalões onde será enquadrado o equipamento afectado por alguma acção destruidora, e assim atribuir custos separados para cada uma delas:

a) Indisponibilidade de equipamento por um período curto (menos de uma semana).

b) Indisponibilidade de equipamento por um período médio (entre uma e duas semanas).

c) Indisponibilidade de equipamento por um longo período (mais de 2 semanas)

e) Perca permanente ou destruição.

CAPÍTULO IV

ATAQUES BEM SUCEDIDOS

Os gestores de sistemas informáticos que estejam ligados à *Internet* devem estar sempre atentos à eventualidade de um ataque poder ser bem sucedido. Não existem sistemas invioláveis, por muito sofisticados que sejam. O que faz com que muitos sistemas não sejam atacados é o facto de o tempo e esforço necessários para violar tais sistemas ser tão elevado que acaba não compensando ataca-los.

O presente capitulo apresenta formas de se detectar ataques bem sucedidos e os procedimentos a seguir(modo de recuperação) perante tal cenário.

4.1 DETECÇÃO DE ATAQUES

É importante que os gestores das redes saibam como agir, após ter sido detectada a ocorrência de situações anómalas que possam ter sido causadas por um atacante. Três regras importantes devem ser seguidas(*Garfinkel e Spafford,1996*):

REGRA 1

Após a ocorrência de um ataque, os gestores da rede são confrontados com uma série de situações e interrogações. Independentemente do que tiver acontecido, qualquer acção a tomar deve ser devidamente planejada. Isto implica ter uma resposta clara a um determinado número de questões que irão determinar quais as acções a serem tomadas:

- Se existiu de facto um ataque ao sistema.
Algo que aparente ter sido causado por um atacante, pode ser resultado de algum erro humano ou falha do *software.*

- Se houve alguma destruição de dados ou equipamento.
O atacante pode conseguir introduzir-se no sistema, mas não conseguir (ou não ser sua intenção) provocar qualquer destruição ou alteração na informação armazenada e/ou configuração do equipamento de comunicação.

- Se é importante obter provas que possam ser usadas nas investigações.

- Se é imprescindível que o sistema volte ao seu normal funcionamento o mais rápido possível.

- Se poderá ter consequências negativas o facto de o incidente vir a ser de conhecimento interno (da organização) e eventualmente externo.

- Se existe o risco de que este incidente volte a acontecer.

REGRA 2

É necessário tomar anotações sobre todas as situações detectadas, incluindo sempre a data e hora de ocorrência através dos registos de translações do sistema. Sempre que forem analisados ficheiros de texto, devem ser impressas cópias destes .

Tendo em mão esta informação, para posterior análise, pode permitir que se economize muito tempo, especialmente quando existe a preocupação de repor o sistema no seu normal funcionamento com brevidade.

REGRA 3

Um factor determinante para conseguir uma resposta efectiva em caso de emergência é a elaboração, prévia, de um plano de acções a seguir:

Identificação e compreensão do problema
O conhecimento do problema com que se esta a lidar é fundamental para se poder tomar acções para o conter.

Suster a acção do atacante
Uma vez identificado o problema, o próximo passo é conter o ataque. Por exemplo, uma vez detectado um utilizador que tem eliminado ficheiros do sistema, a acção imediata a ser tomada é desactiva-lo do sistema, de modo a que este nunca mais possa aceder a qualquer ficheiro.

Confirmação do diagnostico e avaliação de impacto
Após suster o atacante, é necessário confirmar o diagnóstico inicial do ataque e os estragos causados pelo atacante.

Eliminar as causas do acidente
Se a situação ocorrida se deveu à fraquezas na segurança do sistema, será necessário fazer alterações antes que o sistema seja restaurado. Se a causa foi um erro humano, então terão que ser realizadas acções de educação, de modo a que tal não volte a ocorrer

Restaurar o sistema
Depois de conhecida a dimensão e o impacto do ataque, é necessário restaurar o sistema para um estado consistente. Este processo pode ser conseguido usando os *backups* do sistema ou fazendo um simples *restart* do mesmo.

4.2 DETECÇÃO DE INTRUSOS

Existe uma variedade de formas e programas para se detectar intrusos, tais como os pacotes *Tiger* e *Tripwire* especialmente desenhados para esse fim. A acção de verificação da ocorrência de ataques deve ser de forma periódica mas aleatória, de modo a que os atacantes não possam encobrir os seus rastros. Deste modo se garante a *Imprevesibilidade*, princípio básico de segurança.

Segundo *Garfinkel e Spafford(1996)* algumas situações em que se podem detectar intrusos:

- Deduzindo que um ataque possa ter acontecido, baseada em inesperadas alterações ao sistema.

- Recebendo uma mensagem de um administrador de outro sistema indicando a ocorrência de estranhas actividades no seu *site*, proveniente de alguma máquina do nosso sistema.

- Ocorrência de estranhas actividades no sistema ,como quebras de funcionamento, grande actividade do disco, *reboots* inexplicáveis, entre outras.

- Detectando o atacante em flagrante acção. A forma mais simples de o fazer é detectando actividades absolutamente inesperadas:

- Um utilizador que esteja conectado (por linhas *dial-up)* mais que uma vez.

- Um utilizador que não sendo programador, mas que esteja constantemente a executar *compiladores* ou *debuggers*.

- Um utilizador que esteja a executar actividades que sobrecarreguem exageradamente e de forma incaracterística a rede.

- Um utilizador que inicialize várias chamadas simultâneas a sistemas externos.

- Um utilizador que esteja a executar comandos, fazendo-se passar por *superuser*.

- Conexões de máquinas desconhecidas, ou *sites* que , por algum motivo, estejam proibidos.

- Um utilizador que estando de férias, ou que em horas pouco comuns (por ex. de madrugada), tente aceder ao sistema.

O sistema operativo *Unix* possui vários comandos (*finger, users, whodo, w* e *who*) que permitem monitorar a actividade dos utilizadores no sistema. Tais comandos devem ser executados com frequência , pelos administradores do sistema. Após algum tempo será possível associar certos utilizadores à determinadas actividades no sistema.

Deste modo, quando estes utilizadores começam a realizar (com frequência) actividades fora dos parâmetros habituais, um cuidado especial deve ser tomado sobre eles.

CAPÍTULO V

CASO DE ESTUDO:

PROPOSTA DE POLITICA DE SEGURANÇA E *FIREWALL* PARA O BCI

O debate sobre as vantagens de se tornar possível a realização de investimentos seguros e transacções bancárias por parte das instituições financeiras, é quase um assunto do passado.

A *Internet* surge como a arena chave da competição em termos de serviços financeiros no presente. agora, a corrida por rendimentos, busca de mercados e concorrência on-line tomou forma irreversível.

Um estudo realizado pelo *American Bankers Association*, estima que as transações financeiras por *Internet* (*Homebanking*) tiveram um incremento de 600% somente no período entre 1995 e 1998. Estimativas apontam para que até ao ano de 2002, os bancos (só nos Estados Unidos) atinjam despesas anuais superiores 1 bilião de dólares, só com a sua presença na *Internet* e um número superior a 15 milhões de transacções. (Cronin, 1998).

Em Moçambique as instituições financeiras começam também a enveredar pelo caminho da *Internet* e comércio electrónico. Assim muitas destas instituições já estão a construir as suas páginas e a disponibilizar serviços de *homebanking.*

É nesta óptica que o BCI tem o projecto de criação, à médio prazo, da sua página de *Internet*, que para além de permitir obter informações sobre a própria instituição e de carácter financeiro, permitira também realizar transacções (*homebanking).* Assim, será necessária a existência de uma política de segurança que, implementada, garanta a segurança do sistema. A implementação passara pela construção de um *Firewall.*

Para a elaboração desta proposta foram realizadas entrevistas a administradores do Banco, administradores do sistema informático e consulta à bibliografia especializada , sempre tendo em perspectiva o facto de que a politica a elaborar não deve comprometer os objectivos comerciais da instituição.

O presente capítulo apresenta a política de segurança proposta para o BCI. Nele são indicadas as obrigações e deveres dos utilizadores, o modo de utilização do equipamento informático e da informação do sistema. São também especificadas as restrições ao uso de alguns serviços disponíveis para os utilizadores.

5.1 POLITICA DE SEGURANÇA

O BCI possui uma grande variedade de tecnologias de informação e recursos em forma de aplicações informáticas, dados e *hardware*. O valor desta tecnologia é acrescido pela efectiva utilização dos mesmos.

O controle de acessos , o uso dos sistemas e dados deverão estar de acordo com a missão, as políticas e procedimentos do BCI.

O acesso ao sistema e a informação deve apenas ser concedido, aos utilizadores autorizados, para a realização específica das suas actividades.

5.1.1 OBJECTIVOS DA POLITICA

a) Criar mecanismos que permitam estabelecer e manter uma efectiva e adequada salvaguarda das tecnologias de informação para garantir confidencialidade, integridade e disponibilidade dos dados em todos os sistemas informáticos do BCI.

b) Proteger a informação através da:

- Proibição do acesso não autorizado aos recursos do BCI.

- Restrição dos legítimos utilizadores, apenas, aos dados e recursos necessários para a realização da suas actividades.

c) Preservar a confiabilidade, disponibilidade e integridade dos dados, para garantir que os mesmos sejam precisos e relevantes de modo a providenciar suporte à actividade bancária e alcançar as exigências comerciais e administrativas.

d) No caso de ocorrência de constrangimentos , garantir que os serviços solicitados estejam disponíveis para os utilizadores autorizados, ao mesmo tempo que é recusado o acesso aos utilizadores não autorizados.

5.2 ESFERA DE ACÇÃO

5.2.1 APLICAÇÃO DA POLITICA

Esta política devera ser aplicada a todos os empregados , funcionários e utilizadores autorizados que acedam a aplicações, rede e facilidades de apoio ao funcionamento, pertença do BCI.

5.3 PRINCÍPIOS ORIENTADORES

- Os interesses dos clientes devem estar salvaguardados, no caso de ocorrência de danos que afectem a disponibilidade, confidencialidade e integridade dos dados.

- A segurança de Informação deve-se aplicar à todas as plataformas e redes.

- Deve ser alcançado um nível de segurança de informação que não entrem em conflito com as exigências comerciais.

5.4 RESPONSABILIDADES

5.4.1 DIRECÇÃO DE SISTEMAS DE INFORMAÇÃO

A direcção de sistemas de informação tem a seguinte responsabilidades:

- Identificar todos os pontos de exposição(pontos vulneráveis), que resultem de deficiências ao nível da segurança da informação.

- Fazer recomendações , á administração do BCI, que visem a melhorias na segurança do sistema.

- Elaborar planos, a serem aprovados pela administração, para corrigir deficiências identificadas e os respectivos custos de implementação.

- Desenvolver, implementar e reforçar a política de segurança do BCI.

- Garantir que todas direcções que gerem sistemas e dados localmente, sigam todas as normas respeitantes ao uso de tecnologia e recursos pertencentes ao BCI.

- Garantir que as normas cubram (mas não se limitem a estas) as seguintes áreas de segurança de sistemas:

  Segurança do *Software* e *dados.*
  Acesso fisico ao *Hardware* e meios de comunicação.
  Protecção fisica do *hardware* contra danificação ou perda.

- Cuidados com a segurança da informação e treinamento do pessoal.

- Emitir considerações sobre segurança de informação para o desenvolvimento de aplicações ou aquisição de *Software*.

- Rever periodicamente as permissões de acesso dos utilizadores autorizados, para determinar a necessidade de as manter.

- Garantir que as aplicações e a informação são apenas acedidas por utilizadores autorizados e que destes necessitem para realizar as suas actividades profissionais.

- Garantir que as políticas de segurança a implementar não coloquem em risco os objectivos comerciais do BCI.

Os gestores do sistema de informação são também responsáveis por garantir:

- Que alegadas lacunas na segurança do sistema sejam devidamente investigadas.

- A elaboração de planos de contingências e de recuperação de casos de desastres para os diversos tipos de componentes das infra-estruturas do BCI, tal como o *hardware*, rede, etc...

- Alterações no *hardware*, *software*, e outras facilidades do sistema, sejam monitorados para garantir que a segurança não seja comprometida.

5.4.4 UTILIZADORES AUTORIZADOS

São responsabilidades e obrigações dos utilizadores autorizados:

- Compreender e obedecer as políticas e procedimentos de segurança do BCI.

- Participar na elaboração dos planos de segurança da organização.

- Reportar as lacunas de segurança.

- Obedecer a todas as regras e políticas de segurança.

- Não infringir ou tentar infringir as normas de segurança da instituição.

- Não colocar em causa a integridade do equipamento a sua disposição. Proteger adequadamente os recursos em sua posse

- Garantir que os recursos do BCI não são usados para criar, transmitir, armazenar ou copiar informação pornográfica, e outros que não sejam para uso em trabalho.

- Reportar potenciais falhas ou limitações do sistema.

5.5 PROPRIEDADE DA INFORMAÇÃO E APLICAÇÕES

Todos os ficheiros de dados e aplicações produzidas usando recursos do BCI são pertença do banco.

5.6 SERVIÇOS AUTORIZADOS

- Serviço de Correio Electrónico, com algumas restrições a implementarem pelos gestores da rede.

- Serviços de *Web*, com algumas restrições a implementar pelos gestores da rede.

- Serviços de Transferência de Ficheiros, com algumas restrições a implementar pelos gestores da rede.

- Qualquer outro serviço está proibido. As excepções deverão ser discutidas (caso a caso) entre os gestores e a administração e autorizados por esta.

A REDE

Fig.2 A rede usada na implementação do *Firewall*

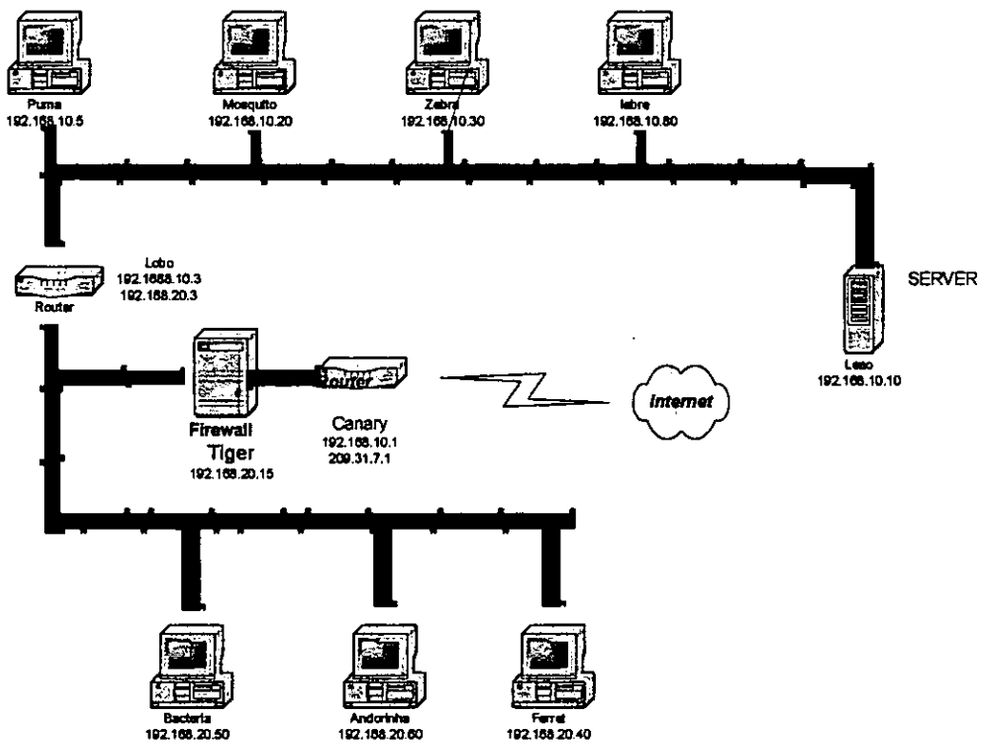


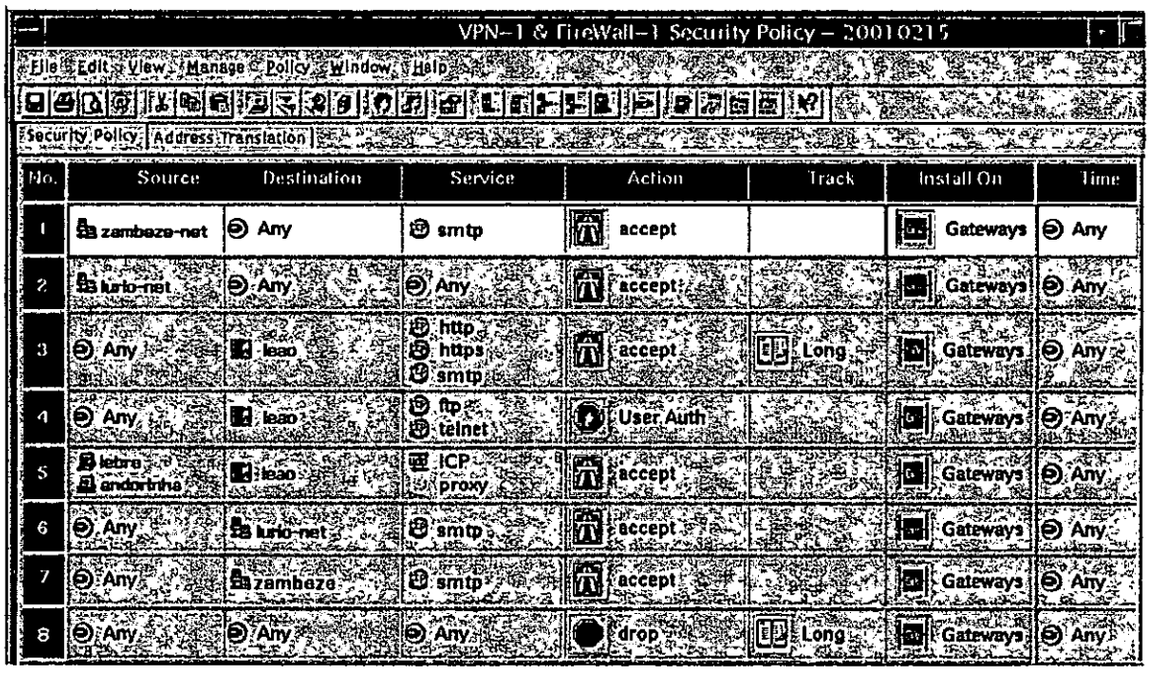
Tabela 3: Componentes da rede

Componente	*Software*
Puma	MS Windows NT Workstatio 4.0, Service Pack 4, Sub-Rede zambeze
Mosquito	Ms Windows NT Workstation 4.0, Service pack 4,Sub-Rede Zambeze
Zebra	MS Windows NT Workstation,Sub-Rede Zambeze
Krill	Linux 5.2, Sub-Rede Zambeze
Leao	Ms Windows NT Server 4.0,Service Pack 4,Sub-Rede Zambeze
Tiger	Windows NT, Firewall –1, Sub-Rede Zambeze
Bactéria	Ms Windows 2000, Sub-Rede Lúrio
Fungi	Ms Windows 2000, Sub-Rede Lúrio
Ferret	Ms Windows 2000, Sub-Rede Lúrio

O FIREWALL

Para a construção do *Firewall,* será usado um computador *Pentium III* de 450 MHZ, 250 de RAM e 15G de disco. O *Software* será o FIREWALL-1 (VPN-1).

A configuração consiste, na sua parte mais importante, por oito regras que determinam o tratamento que o *Firewall* deverá dar sempre que for solicitado um serviço na rede:



DESCRIÇÃO DAS REGRAS DO FIREWALL:

Regra 1 : Partindo da rede Zambeze para qualquer destino, o serviço *smtp* esta sempre autorizado a qualquer hora .

Regra 2 : Da rede Lúrio para qualquer destino, estão autorizados todos os serviços a qualquer hora

Regra 3 : De qualquer destino para o servidor *Leão* estão autorizados os serviços *http, https* e *smtp* a qualquer hora.

Regra 4 : De qualquer destino para o servidor *Leão,* estão autorizados os serviços *ftp e telnet* mediante autenticação dos usuários a qualquer hora.

Regra 5 : Dos *Workstations Lúrio* e *Andorinha* para o servidor *Leão,* estão autorizados os serviços de *Proxy* e *ICP* a qualquer hora .

Regra 6 : De qualquer destino para a rede *Lúrio,* esta autorizado o serviço *smtp* a qualquer hora .

Regra 7: De qualquer destino para a rede *Zambeze,* esta autorizado o serviço *smtp* a qualquer hora.

Regra 8 : Qualquer outro serviço não definido anteriormente, de e para qualquer outro destino são sempre recusados.

CAPÍTULO VI

CONCLUSÕES E RECOMENDAÇÕES

A segurança não está associada apenas a um sistema, dispositivo ou configuração específica, mas sim a todo um conjunto de variáveis interdependentes, de tal modo que ela será tão forte quanto mais forte for o seu ponto mais vulnerável.

Para se implementar um sistema seguro, é necessário conhecer as suas vulnerabilidades, os ataques que pode sofrer e as formas de os combater. A segurança é comparável à arte da guerra, onde, para alcançar os objectivos é necessário conhecer o inimigo, conhecermo-nos a nós próprios, saber quando, como e por onde o inimigo pode atacar e quando, como e onde nos defendermos dele.

A segurança de um sistema está directamente relacionada com a sua funcionalidade. Quanto maior for a segurança de um sistema, menor será a sua funcionalidade e vice-versa. Por este motivo, ao serem elaborados mecanismos e políticas de segurança deve-se ter sempre a preocupação de não comprometer a funcionalidade do sistema, de modo a não se colocar em causa os objectivos comerciais da instituição. Deverão ser encontrados pontos de equilíbrio entre as necessidades de segurança e o nível de funcionalidade exigidos para o sistema.

É sempre recomendável a adopção de políticas de negação por defeito em detrimento da aceitação por defeito, mesmo tendo em conta que a segurança é inversamente proporcional ao desempenho

As grandes empresas e instituições, tendem a preocupar-se mais com as situações de risco que possam vir do exterior das suas redes, descurando o perigo vindo do interior. Os utilizadores internos, quando mal treinados (ou mal intencionados) no uso das ferramentas ao seu dispor , são o principal factor de risco que pesa sobre as organizações. Deve ser norma da instituição a implementação de programas de formação aos seus utilizadores e a promoção de acções tendo em vista sensibilizar os mesmos para a importância de se respeitarem as regras e políticas de segurança aprovadas.

Uma vez que é praticamente impossível conceber sistemas invioláveis, é importante a existência de fortes mecanismos de auditoria, controlo e recolha de provas (das acções criminosas). Por outro lado, como acção complementar, deve existir legislação que proteja em termos jurídicos as organizações e que sirva de factor de dissuasão a actos de crime informático, apesar de no mundo da informática ser mais complicado implementar tal legislação, uma vez que o crime muitas vezes é praticado sem a presença física do atacante ou mesmo a partir de outras zonas de jurisdição.

As topologias das redes a serem implementadas são muito importantes na implementação de políticas de segurança. É recomendável a adopção de topologias que permitam evitar ataques de *sniffers*, principalmente. A criptografia deve ser usada como complemento ao uso das topologias a adoptar, pois existe sempre a possibilidade de que os pacotes trocados na rede sejam

interceptados. Deste modo a tarefa do atacante fica mais dificultada. Os utilizadores devem ser sensibilizados para a necessidade de encriptar a informação que é trocada.

BIBLIOGRAFIA

Chapman, D. Brent and Zwicky, Elizabeth D. (1995). Building Internet Firewalls, 1st Edition, California, United States, O' Reilly.

Cronin, Mary J.(1998).Banking and Finance On The Internet. 1st Edition, New York, Wiley & Sons.

Garfinkel, Simson and Spafford, Gene (1999). Comercio e Segurança na Web, Market Books.

Garfinkel Simson, and Spafford, Gene (1996). Pratical Unix & Internet Security, 2nd Edition, California, United States, O'Reilly.

Kaufmann, Philip(2001). Computer Crime – Major Risks. Conferência Internacional , Maputo, Centro de Informática da UEM.

Larson, Eric & Stephens, Brian (1999). Web Servers, Security, & Maintenance, 1st Edition, London, U.K, Prentice Hall.

Seberry, J. (1989). Cryptography – An Introduction to Computer Security, Prentice Hall.

Stein, Lincoln D. (1998). Web security- A Step By Step Reference Guide, Addison Wesley.

Pistelli, D. Criptografia : http:/www.nucc.pucsp.br/novo/cripto/cripto.html – ultima consulta em Novembro de 2001.

Secure Socket Layer : http:/home.it.netscape.com/products/security/ssl/inde – ultima consulta em Janeiro de 2002.

Network Wizard : http:/www.nw.com – ultima consulta em Janeiro de 2002

GLOSSÁRIO

ARP(Adress Resolution Protocol): Protocolo que mapeia endereços de IP para endereços físicos.

AUTENTICATION SERVER PROTOCOL: Serviço de autenticação baseado em TCP, que pode verificar a identidade de um usuário.

BACKUP: Preservar um sistema de arquivos ou arquivos, normalmente para a recuperação pós desastre.

BUG: Brecha ou fraquesa de um programa de Computador.

CERTIFICADO DIGITAL: Qualquer valor digital utilizado em um procedimento de autenticação. Em geral são valores numéricos , derivados de processos criptográficos .

FLOOD: Ferramentas que destroem a fila de conexões de um sistema compatível com TCP/IP, causando assim negação de serviços.

GATEWAYS: Dispositivo do *firewall* que desactiva a comunicação directa entre o mundo externo e a rede interna.

HACKER: Profundo conhecedor de computadores e áreas de computadores.

CRACKER: *Hacker* mal intencionado.

IDEA: Algoritmo criptográfico que opera com uma chave de 128 bits por padrão.

TCP/IP-*Transmission Control Protocol/Internet Ptrotocol-*

USERID: Palavra que permite identificar um utilizador que pretenda conectar-se a um determinado sistema.

HTTP-*Hiper Text Transfer Protocol-* protocolo utilizado para o tráfego de hipertexto através da *Internet*, e o protocolo subjacente da *WWW.*
dados e Internet.

ROUTERS – Dispositivos usados para conectar(rotear pacotes) redes de diferentes tipos. são em certos contextos conhecidos como GATEWAYS.

SNIFFER: Programa que sub-repticiamente captura data gramas através de uma rede. Ele pode ser usado legitimamente por um administrador da rede que tenta diagnosticar problemas nesta, ou por um *Cracker* que tenta descobrir nome de usuários e senhas.

MODEM (Modulador/Demodulador) – Dispositivo que traduz dados seriais em sons e sinais analógicos que podem ser transmitidos por linhas telefónicas.

HUB – Aparelho com uma série de portas RJ-45, às quais são ligados os cabos de rede provenientes de cada um dos computadores. Permite a interligação dos computadores na rede.

CERTIFICADO DIGITAL – Cartões digitais que permitem identificar a identidade do seu detentor. Contem o nome, a sua chave pública, um número serial e os prazos de emissão e validade do certificado.

ANEXOS

ANEXO 1

Tabela 1: Pacotes comuns de bombas de correio electrónico e nomes de arquivos associados

Pacote de bomba	*Nome de arquivo*
Up Yours	UPYOURS3.ZIP,UPYOURS3.EXE,MAILCHECK.EXE,UPYOURSX·
Kaboom	KABOOM3.ZIP,KABOOM3.EXE,KABOOM3!.ZIP,WSERR.DLL
The Unabomber	UNA.EXE,KWANTAM.NFO
The Windows Email Bomber	BOMB.EXE,BOMB.TXT,BOMB02B.ZIP
Gatemail	GATEMAIL.C
Unix Mailbomber	MAILBOMB.C

ANEXO 2

Tabela 2: Aplicativos de filtragem de correio e suas localizações

Pacote de filtragem	*Localização*
Stalker	http://www.stalker.com/
Eudora Mail Server)	http://www.eudora.com/
Musashi	http://www.sonosoft.com/musashi/index.html
Advenced E-mail Protector	http://www.antispam.org
E-mail Chomper (Win 9x)	http:/www.sarum.com/echomp.html
Spam Buster(Win 9x)	http:/www.contactplus.com/