UNIVERSIDADE FEDERAL DE SANTA CATARINA

Engenharia de Produção e Sistemas

UM MODELO PARA SEGURANÇA E DISPONIBILIDADE DE INFORMAÇÕES EM UM SISTEMA DE REDE DISTRIBUIDO

Orientadora: Profª. Elisabeth Sueli Specialski

Aluno: Rogerio Domingos Hining

Florianópolis

Santa Catarina – Brasil

Setembro de 2000

Rogerio Domingos Hining

UM MODELO PARA SEGURANÇA E DISPONIBILIDADE DE INFORMAÇÕES EM UM SISTEMA DE REDE DISTRIBUIDO

"Trabalho de dissertação apresentado ao Departamento de Engenharia de Produção e Sistemas (EPS) área de Mídia e Conhecimento da Universidade Federal de Santa Catarina (UFSC), como requisito para obtenção do Título de Mestre em Engenharia de Produção e Sistemas."

Orientadora: Profª. Elisabeth Sueli Specialski

Florianópolis
Santa Catarina - Brasil
Setembro de 2000

Rogerio Domingos Hining

UM MODELO PARA SEGURANÇA E DISPONIBILIDADE DE INFORMAÇÕES EM UM SISTEMA DE REDE DISTRIBUIDO

Este trabalho de dissertação foi apresentado ao Departamento de Engenharia de Produção e Sistemas (EPS) área de Mídia e Conhecimento da Universidade Federal de Santa Catarina (UFSC), e foi julgado adequado para a obtenção do Título de **Mestre em Engenharia de Produção e Sistemas**

Profª Elizabeth Sueli Specialski, Dra
Orientadora, UFSC

Profº Ricardo Miranda Barcia, PhD.
Coordenador Curso, UFSC

Banca Examinadora

Profª Elizabeth Sueli Specialski, Dra
Orientadora, UFSC

Profº João Bosco da Mota Alves, Dr.
Membro da Banca, UFSC

Profº Luiz Fernando Jacintho Maia, Dr.
Membro da Banca, UFSC

O saber não é como nós comumente chamamos "um tipo de conhecimento", o sábio não é um sujeito que conhece muitas coisas, mas um sujeito que tem uma habilidade muito peculiar de perceber uma ocorrência, avaliar essa ocorrência, tomar uma decisão em relação a essa ocorrência e agir em resposta a essa ocorrência, tudo de forma correta.

A sabedoria consiste em perceber, avaliar, decidir e agir de forma correta.

Isso não é privilégio de diplomados, nem de pessoa que tenha formação superior, erudição, nada disso.

Isso é privilégio apenas de alguém que desenvolveu a capacidade de ouvir a voz interior.

A capacidade de ouvir o seu próprio mestre interior.

A voz do espírito, a voz do silêncio. Esse indivíduo que escuta essa voz, e segue essa orientação e que decide e age da forma correta é o sábio.

Helena Petrovna Blavatsky

Agradecimentos

A Deus, fonte de força e perseverança, requisitos indispensáveis para alcançar este objetivo.

A minha família, especialmente a Josiane e ao Lucas pela compreensão, apoio e confiança, e a toda a grande família que incentivou e colaborou das mais diversas formas.

Ao meu grande amigo Davidson pela ajuda, apoio e incentivo.

Aos professores Bosco e Beth, meus desorientadores, que sabem como ninguém incentivar, motivar e fazer produzir resultados. A amizade conquistada certamente trará novas alegrias, como as muitas que tivemos em conjunto.

Aos professores Maia e Mazzucco, e em seus nomes a todos os nossos mestres, pois todos tiveram sua parcela de contribuição neste trabalho.

A Universidade do Oeste de Santa Catarina (UNOESC – São Miguel) e a Universidade Federal de Santa Catarina (UFSC) que tornaram possível esta importante conquista.

A todos vocês meus sinceros agradecimentos !

Sumário

Lista de Figuras

Resumo

A segurança de redes merece muita atenção por parte de administradores de redes, principalmente com as crescentes tentativas de invasão e ataques noticiados diariamente. A maior característica de uma rede de computadores é a alta disponibilidade de informações, principalmente aliando uma rede corporativa à Internet, porém, esta nova funcionalidade traz consigo um problema de escala também grandiosa, a falta de segurança dos modelos distribuídos de redes, ou seja, quanto maior a disponibilidade menor a segurança. Esta dicotomia entre a total disponibilidade de informações e a efetiva segurança de redes é o objeto deste trabalho. Procuramos construir um modelo para uma rede distribuída que contemple níveis de segurança viáveis e a maior disponibilidade de informações possível. Para esta construção, apresentamos inicialmente alguns conceitos importantes sobre redes de computadores, na seqüência, os conceitos de segurança e a apresentação do estudo de caso e modelo proposto.

Abstract

The safety of nets deserves a lot of attention on the part of administrators of nets, mainly with the growing invasion attempts and attacks informed daily. The largest characteristic of a net of computers is the high readiness of information, mainly forming an alliance a corporate net with the Internet, even so, this new functionality brings a huge scale problem, the lack of safety of the distributed models of nets, that is to say, as larger the smaller readiness the safety. This dicotomy enters to total readiness of information and the effective safety of nets is the object of this work. We tried to build a model for a distributed net that contemplates viable levels of safety and the largest possible readiness of information. For this construction, we presented some important concepts initially on nets of computers, in the sequence, safety's concepts and the presentation of the case study and proposed model.

Introdução

Devido ao grande crescimento da Rede UNOESC – São Miguel, e a demanda crescente de informações nos diversos segmentos da instituição, deparamo-nos com um sério problema – Como disponibilizar informações da maneira mais abrangente possível sem perder a segurança, tanto de sistemas quanto destas informações?

É de consciência geral a dicotomia da total segurança de redes e total disponibilidade de informações, desta forma pretendemos construir um modelo que permita o maior nível de disponibilidade com o melhor índice de segurança possível.

Este documento está estruturado em seis tópicos a seguir:

O primeiro tópico apresentamos os conceitos básicos sobre os temas relevantes deste estudo, como redes de computadores, suas classificações e arquiteturas, invasões a sistemas computacionais, hackers, crackers, ferramentas de proteção de redes.

No segundo tópico, discorremos sobre os conceitos específicos da segurança de redes, métodos globais e específicos de proteção, disponibilidade, minimização das invasões.

O estudo do caso da Rede UNOESC – São Miguel apresenta-se no quarto tópico, demonstrando o histórico da Rede UNOESC, seu crescimento ao longo de sua história, seu formato atual e infraestrutura. Neste momento, demonstra-se o modelo proposto para solução do problema apresentado.

No quinto tópico colocamos as conclusões a que chegamos e sugestões para trabalhos posteriores que possam complementar e dar prosseguimento a este estudo.

Nos anexos temos alguns documentos que mostram as diversas faces do submundo das invasões e ataques a sistemas computacionais.

1 Conceitos Básicos

1.2 Redes de Computadores

A história nos mostra que cada um dos últimos séculos foi dominado por uma tecnologia diferente. A revolução industrial no século XVIII, as máquinas a vapor no século XIX e a tecnologia da informação no século XX. Exemplos disto são as redes de telefonia em escala mundial, o rádio, a televisão, os computadores e os satélites de comunicação. Com estas conquistas, o conceito de distância geográfica tornou-se, em alguns casos, um fator pouco importante para a solução de problemas.

Apesar da indústria da informática ser muito jovem se comparada a outros setores (a de automóveis e de aviões, por exemplo), os progressos ocorridos foram espetaculares em um curto espaço de tempo. Nas duas primeiras décadas de sua existência, os sistemas computacionais eram acondicionados em uma grande sala com paredes de vidro, através das quais a maior parte dos visitantes, e até usuários, podiam contemplar extasiados aquela maravilha eletrônica. Uma empresa de médio porte ou uma universidade contava apenas com um ou dois computadores, enquanto grandes instituições tinham, no máximo, algumas dezenas. Era pura ficção científica a idéia de que, em apenas 20 anos, haveria milhões de computadores muito mais avançados, do tamanho de um selo postal, ou ainda menor.

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais foram organizados. Está totalmente ultrapassado o conceito de "centro de computação" como uma sala onde os usuários levam os programas para serem

processados. Este conceito foi substituído pelas chamadas redes de computadores, nas quais os trabalhos podem ser realizados por uma série de computadores interconectados. Sendo assim, é uma necessidade o conhecimento, por parte do pessoal envolvido com informática, dos conceitos e funcionamento das redes de computadores.

É importante então conceituar o que entendemos por redes de computadores. Nós usaremos o termo rede de computadores para designar um conjunto de computadores autônomos e interconectados. Dois computadores são interconectados quando podem trocar informações através de algum mecanismo de comunicação. Quando dizemos que eles devem ser autônomos desejamos excluir os sistemas onde existe uma clara relação mestre/escravo.

Outro esclarecimento importante é fazer uma clara distinção entre uma rede de computadores e um sistema distribuído. A principal diferença entre eles é que, em um sistema distribuído, a existência de diversos computadores autônomos é transparente para o usuário. A transparência de utilização é dada pelo sistema operacional. Em suma, o usuário de um sistema distribuído não tem consciência de que há vários processadores. Para ele é como se existisse um processador virtual e todas as atividades para execução de uma tarefa acontecem de forma o mais automatizada possível. Por outro lado, em uma rede, o usuário necessita realizar explicitamente suas tarefas, tais como: fazer o *login* em uma máquina, realizar a transferência de seus arquivos, submeter suas tarefas remotas, entre outras. Na prática, um sistema distribuído é um sistema de software instalado em uma rede, proporcionando um alto grau de coesão e transparência ao usuário. É o software, ou o sistema operacional, que determina a diferença entre uma rede e um sistema distribuído, não o hardware. No entanto os dois assuntos possuem uma série de pontos em comum, por exemplo: os sistemas distribuídos e as redes necessitam movimentar arquivos. A diferença está em quem é o responsável pela movimentação: o sistema operacional ou o usuário.

1.2.1 Histórico das Redes de Computadores

A evolução da microeletrônica e da informática tem possibilitado a obtenção de processadores e outros componentes de computadores cada vez mais potentes e velozes, num tamanho mais reduzido e num preço cada vez mais acessível a um maior número de pessoas.

Os microprocessadores existentes hoje em dia, que ocupam o espaço menor do que uma caixa de fósforos, substituem e ultrapassam as capacidades dos computadores de alguns anos atrás, que ocupavam salas inteiras. Estes eram máquinas bastante complexas no que diz respeito á sua utilização, sendo operadas apenas por especialistas. Os usuários daqueles computadores normalmente submetiam seus programas aplicativos como *jobs* (ou tarefas) sem qualquer interação com o processamento do programa.

Uma primeira tentativa de interação com o computador ocorreu no início dos anos 60, com a técnica de *time-sharing*, que foi o resultado do desenvolvimento dos sistemas computacionais e da tecnologia de transmissão de dados. Nesta técnica, um conjunto de terminais era conectado a um computador central através de linhas de comunicação de baixa velocidade, o que permitia aos usuários interagir com os seus programas. A necessidade de conexão de terminais para o processamento interativo foi o ponto de partida para o estabelecimento de necessidades de comunicação nos computadores. A técnica de *time-sharing* permitia a um grande conjunto de usuários o compartilhamento de um único computador para a resolução de uma grande diversidade de problemas e as aplicações desenvolvidas foram cada vez mais se multiplicando e se diversificando (cálculos complexos, produção de relatórios, ensino de programação, aplicações militares, etc). Este aumento na demanda implicava numa necessidade crescente de atualizações e incremento na capacidade de cálculo e de armazenamento nas CPUs, o que nem sempre era viável ou possível, dado que

os computadores do tipo *mainframes* nem sempre eram adaptados para suportar determinadas extensões.

O avanço tecnológico na área dos circuitos integrados, gerando componentes mais poderosos a um custo mais baixo, foi caindo o preço da CPU. Este evento constituiu a chamada revolução do hardware. Nos anos 70, com o surgimento dos minicomputadores, foi possível adaptar as capacidades de processamento às reais necessidades de uma dada aplicação. Além disso, um grande número de usuários operavam sobre conjuntos comuns de informações, gerando a necessidade de compartilhamento de dados, de dispositivos de armazenamento e de periféricos entre os vários departamentos de uma empresa. Isto deu um novo impulso aos trabalhos no sentido de resolver os problemas de comunicação entre os computadores. Este novo tipo de aplicações exigia velocidade e capacidade de transmissão muito mais elevadas que no caso da conexão de terminais a um computador central. Assim, com a utilização de minicomputadores interconectados, obtinha-se muitas vezes uma capacidade de processamento superior àquela possível com a utilização dos *mainframes*. Outro aspecto interessante é que as redes podiam ser estendidas em função das necessidades de processamento das aplicações. Além disso, a modularidade natural das redes de computadores era tal que uma falha num minicomputador ou na rede tinha um efeito bastante limitado em relação ao processamento global.

O surgimento dos minicomputadores e dos computadores pessoais trouxe uma nova solução para o problema de máquinas multi-usuário pois dava uma CPU para cada um deles. As pequenas companhias e as subsidiárias utilizavam-se dos minicomputadores para algum processamento local e na preparação dos dados para o *bureaux* de serviços ou para a matriz. Os dados eram transferidos quando exigiam um grande volume de processamento ou um processamento requerendo software ou hardware especial.

O uso dos minicomputadores minimizou mas não solucionou o problema da comunicação. Minimizou porque os dados podiam agora ser preparados e armazenados em fita magnética e transportados via sistema de malotes. Este sistema de transporte não é, obviamente, o mais adequado para transferência de informação pois está sujeito a acidentes, gerando atraso ou perda total do material.

Por outro lado, o sistema centralizado oferecia a vantagem de compartilhar recursos caros tanto de software como de hardware, ou seja, o software e hardware especial era caro mas seu preço era amortizado pelo rateio do custo dos periféricos entre os vários usuários. Surge, então, a necessidade de uma nova tecnologia para compartilhamento de recursos.

Paralelamente, a tecnologia de comunicações alcançava a transmissão digital em linhas telefônicas através de *modems*. Este serviço era caro e apenas suportado por grandes companhias, uma vez que utilizavam linhas telefônicas de forma dedicada. Esta situação perdurou por algum tempo (no Brasil, até março de 1985) e era necessária outra solução para comunicação através de uma nova tecnologia de comunicação.

A necessidade da disseminação da informação e os avanços em tecnologia de armazenamento, propiciaram o aparecimento de discos de grande capacidade e mais baratos (explosão da informação e grandes bancos de dados). Aí o problema de comunicação tornou-se muito mais sério. Para acessos não muito freqüentes, uma linha telefônica dedicada não era viável em termos de custo e o transporte via malote era inviável em termos de velocidade. A solução para o compartilhamento de recursos físicos e lógicos juntamente com a vantagem de se ter um sistema descentralizado, só pode ser alcançada através da interconexão das CPUs entre si. É a isso que se propõem às redes de computadores.

As soluções encontradas, na época, para a comunicação de computadores em termos de longa distância foi à tecnologia de comutação de pacotes, que solucionou o problema da linha telefônica dedicada e o problema do transporte via malote. Num ambiente restrito a uma região local (por exemplo, uma fábrica, um campus), o problema do compartilhamento de recursos através de interconexão de CPUs foi resolvido através da tecnologia de redes locais.

Atualmente, as vantagens dos sistemas distribuídos e interconectados são uma evidência reconhecida para as aplicações mais diversas, desde a automação de escritórios até o controle de processos, passando por aplicações de gerenciamento bancário, reservas de passagens aéreas, processamento de texto, educação à distância, correio eletrônico, WWW, entre outras tão bem conhecidas.

A junção de duas tecnologias – comunicação e processamento de informações – veio revolucionar o mundo em que vivemos, abrindo as fronteiras para novas formas de comunicação, e permitindo maior eficácia dos sistemas computacionais. As redes de computadores são uma realidade neste nosso contexto atual.

1.2.2 Importância das Redes de Computadores

Um grande número de empresas possui atualmente uma quantidade relativamente grande de computadores operando nos seus diversos setores. Um exemplo deste fato é aquele de uma empresa que possui diversas fábricas contendo cada uma um computador responsável das atividades de base da fábrica (controle de estoques, controle da produção e produção da folha de pagamentos). Neste exemplo, apesar da possibilidade de operação destes computadores de maneira isolada, é evidente que sua operação seria mais eficiente se eles

fossem conectados para, por exemplo, permitir o tratamento das informações de todas as fábricas da empresa. O objetivo da conexão dos diferentes computadores da empresa é permitir o que poderíamos chamar de compartilhamento de recursos, ou seja, tornar acessíveis a cada computador todos os dados gerados nas diversas fábricas da empresa.

Um outro ponto importante da existência das Redes de Comunicação é relacionado a um aumento na confiabilidade do sistema como um todo. Pode-se, por exemplo, ter multiplicados os arquivos em duas ou mais máquinas para que, em caso de defeito de uma máquina, cópias dos arquivos continuem acessíveis em outras máquinas. Além disso, o sistema pode operar em regime degradado no caso de pane de um computador, sendo que outra máquina pode assumir a sua tarefa. A continuidade de funcionamento de um sistema é ponto importante para um grande número de aplicações, como por exemplo: aplicações militares, bancárias, o controle de tráfego aéreo, etc.

A redução de custos é uma outra questão importante da utilização das Redes de Comunicação, uma vez que computadores de pequeno porte apresentam uma menor relação preço/desempenho que os grandes. Assim, sistemas que utilizariam apenas uma máquina de grande porte e de custo muito elevado podem ser concebidos à base da utilização de um grande número de microcomputadores (ou estações de trabalho) manipulando dados presentes num ou mais servidores de arquivos. Os *mainframes* são dezenas de vezes mais rápidos do que alguns computadores pessoais mas também seu preço é milhares de vezes maior. Esta situação levou os projetistas a criarem sistemas baseados em computadores pessoais para os usuários com os dados mantidos em um ou mais servidores de arquivos compartilhados, Neste modelo os usuários são chamados clientes e a organização geral é denominada modelo cliente/servidor. No modelo cliente/servidor um processo cliente envia uma mensagem de solicitação ao processo servidor para que alguma tarefa seja executada. Em seguida o

processo servidor executa a tarefa e envia a resposta ao processo cliente. Geralmente existem muitos clientes usando um pequeno número de servidores.

Ainda temos como vantagem no uso das redes a escalabilidade, que é a possibilidade de aumentar gradualmente o desempenho do sistema à medida que cresce o volume de carga, através da adição de mais processadores. Esta era uma enorme dificuldade nos sistemas centralizados. Quando o limite de capacidade era atingido, o sistema tinha que ser substituído por um maior, o que geralmente implicava em altos custos e grandes aborrecimentos para os usuários.

1.2.3 Hardware de Rede

Em relação à estruturação, dois aspectos podem ser abordados: a física e a lógica. Para isso serão discutidas as várias topologias de uma rede. O conceito de topologia, até a pouco relacionado apenas com a estruturação física da rede, agora abrange, também, a forma como a mesma é definida logicamente.

Existem várias classificações para as diferentes redes de computadores. Dentre elas, duas dimensões se destacam mais: a escala e a tecnologia de transmissão.

Basicamente há dois tipos de tecnologia de transmissão: as redes em difusão e as redes ponto-a-ponto. Nas redes em difusão há apenas um canal de transmissão compartilhado por todas as máquinas. Uma mensagem enviada por uma estação é "ouvida" por todas as outras estações. Nas redes ponto-a-ponto existem várias conexões entre pares individuais de estações. Estes dois tipos de ligação podem ser visualizados na figura 1.1 a seguir.

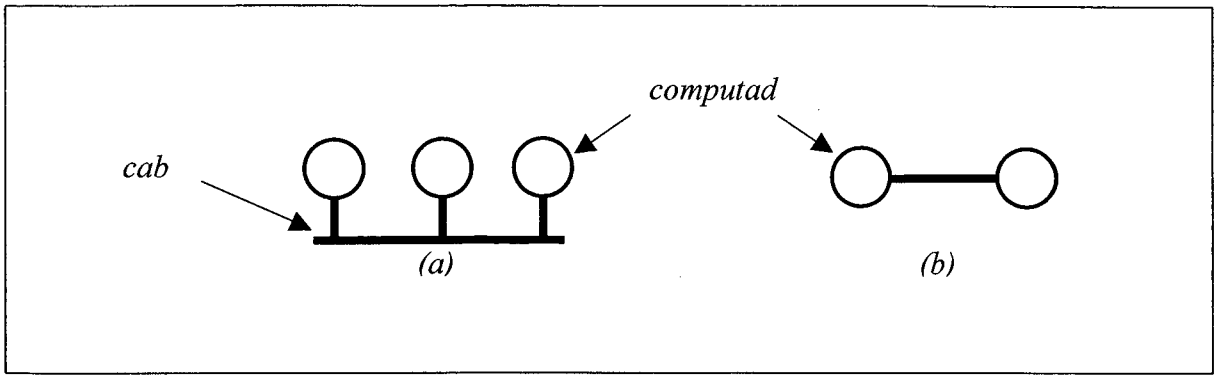

Figura 1.1 – Rede em difusão (a) e rede ponto-a-ponto (b).

1.2.4 As diferentes topologias

Um ponto importante no que diz respeito à concepção de uma rede de comunicação é a definição da maneira como as diferentes estações serão interligadas. Estes arranjos são denominados topologia da rede. Estas topologias estão relacionadas à forma como o canal de comunicação será alocado, ou seja, através de canais ponto-a-ponto ou canais de difusão.

Nas topologias que utilizam canais ponto-a-ponto, a rede é composta de diversas linhas de comunicação, cada linha sendo associada à conexão de um par de estações. Neste caso, se duas estações precisam comunicar-se e não há entre elas um cabo comum, a comunicação será feita de modo indireto, através de uma (ou mais) estações. Assim, quando uma mensagem é enviada de uma estação a outra de forma indireta, ela será recebida integralmente por cada estação e, uma vez que a linha de saída da estação considerada está livre, retransmitida à estação seguinte.

Esta política de transmissão é também conhecida por *store and forward.* A maior parte das redes de longa distância são do tipo ponto-a-ponto. As redes ponto-a-ponto podem ser concebidas segundo diferentes topologias. As redes locais ponto-a-ponto são caracterizadas

normalmente por uma topologia simétrica; as redes de longa distância apresentam geralmente topologias assimétricas. A figura 1.2 apresenta as diferentes topologias possíveis nas redes ponto-a-ponto.

Uma outra classe de redes, as redes de difusão, são caracterizadas pelo compartilhamento, por todas as estações, de um único canal de comunicação. Neste caso, as mensagens enviadas por uma estação são recebidas por todas as demais conectadas ao suporte de transmissão, sendo que um campo de endereço contido na mensagem permite identificar o destinatário. Na recepção, a máquina verifica se o conteúdo do campo de endereço corresponde ao seu e, em caso negativo, a mensagem é ignorada. As redes locais pertencem geralmente a esta classe de redes.

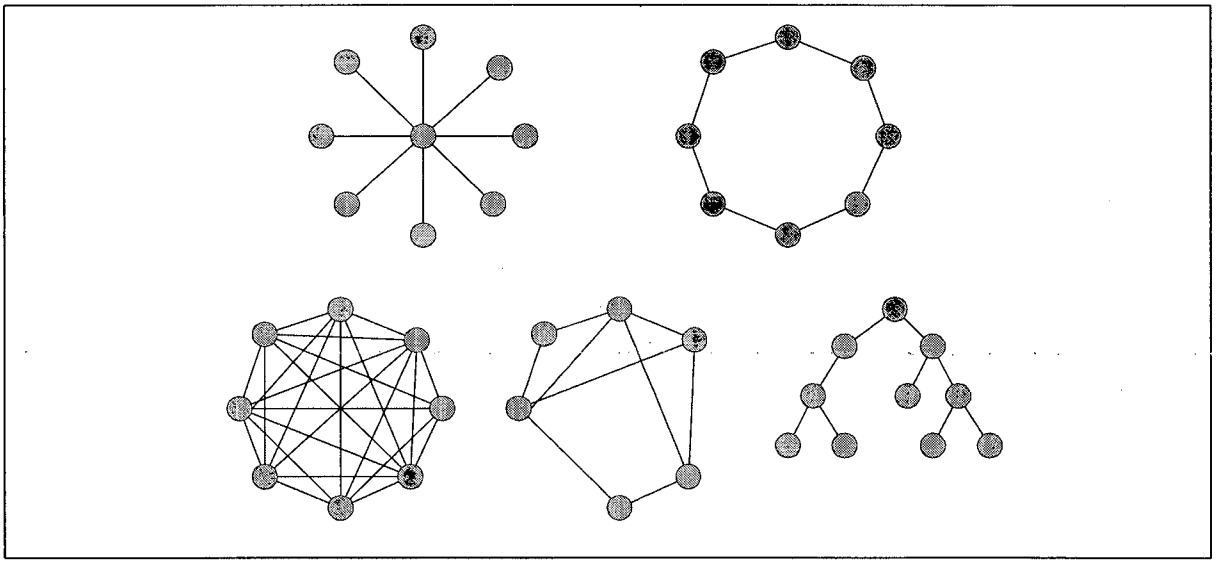

Figura 1.2 - Topologias ponto-a-ponto: estrela, anel, malha regular, malha irregular e árvore.

A figura 1.3 apresenta algumas topologias possíveis no caso das redes em difusão. Numa rede em barramento, uma única máquina pode estar transmitindo a cada instante. As demais estações devem esperar para transmissão caso o barramento esteja ocupado. Para isto, um mecanismo de arbitragem deve ser implementado para resolver possíveis problemas de

conflito (quando duas ou mais estações querem enviar uma mensagem), este mecanismo pode ser centralizado ou distribuído.

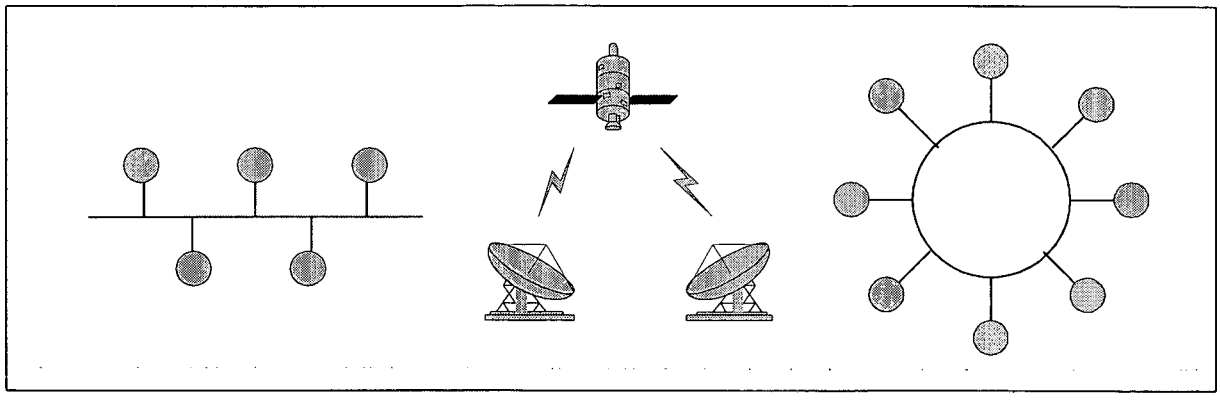

Figura 1.3 - Topologias das redes de difusão: barramento, satélite e anel

No caso das redes de satélite (ou rádio), cada estação é dotada de uma antena através da qual pode enviar e receber mensagens. Cada estação pode "escutar" o satélite e, em alguns casos, receber diretamente as mensagens enviadas pelas demais estações. No caso do anel, cada *bit* transmitido é propagado de maneira independente em relação à mensagem ao qual ele pertence. Em geral, cada *bit* realiza uma volta completa no anel durante o tempo necessário para a emissão de um certo número de *bits*, antes mesmo da emissão completa da mensagem. Também nesta topologia, é necessária a implementação de um mecanismo de acesso ao suporte de comunicação.

1.2.5 Topologia física X topologia lógica

A topologia de uma rede irá determinar, em parte, o método de acesso a rede utilizado. Métodos de acesso são necessários para regular a utilização dos meios físicos compartilhados.

A forte tendência de utilização de *hubs* nas instalações físicas das redes corresponde, fisicamente, a implantação de uma topologia em estrela. Esta tendência é explicada pela crescente necessidade de melhorar o gerenciamento e a manutenção nessas instalações. A topologia em estrela apresenta uma baixa confiabilidade porém os avanços da eletrônica já permitem que se construam equipamentos de alta confiabilidade, viabilizando este tipo de topologia.

A utilização de *hubs* não exige, necessariamente, que as interfaces das estações com a rede o percebam como uma topologia em estrela. O funcionamento continua a ser como no acesso a um barramento ou a um anel, com os seus respectivos métodos de acesso. Sendo assim, podemos diferenciar dois tipos de topologias: uma topologia lógica, que é aquela observada sob o ponto de vista das interfaces das estações com a rede (que inclui o método de acesso), e uma topologia física, que diz respeito à configuração física utilizada na instalação da rede.

A construção dos *hubs* teve uma evolução contínua no sentido de que os mesmos não implementem somente a utilização do meio compartilhado, mas também possibilitem a troca de mensagens entre várias estações simultaneamente. Desta forma as estações podem obter para si taxas efetivas de transmissão bem maiores. Esse tipo de elemento, também central, é denominado *switch*. As redes ATM, por exemplo, baseiam-se na presença de *switches* de grande capacidade de comutação que permitem taxas de transmissão que podem chegar à ordem de Gbps (*gigabits* por segundo).

1.2.6 Categorias de redes

As redes também podem ser classificadas por escala. A figura 1.4 mostra uma classificação das várias redes de computadores em relação a sua abrangência. Basicamente elas podem ser classificadas em três grupos: *LAN – Local Area Network* ou Rede Local, *MAN – Metropolitan Area Network* ou Rede Metropolitana e *WAN – Wide Area Network* ou Rede Geograficamente Distribuída (ou de Longa Distância).

Distância entre nós	Abrangência	
até 10 m	Sala	LAN
até 100 m	Edifício	
até 1 km	Campus	MAN
até 10 km	Cidade	
até 100 km	País	WAN
até 1.000 km	Continente	
até 10.000 km	Planeta	

Figura 1.4- Classificação de redes quanto à distância física entre os nós.

A diferença na dimensão das redes introduz diferentes problemas e necessidades. No que diz respeito ao exemplo de microcomputadores, a rede é classificada como sendo uma Rede Local, caracterizada particularmente por uma pequena extensão, limitando-se normalmente à interconexão de computadores localizados numa mesma sala, num mesmo prédio ou num campus. Este tipo de rede invariavelmente proprietária. Uma alternativa a este tipo de rede, muito utilizada atualmente são as Redes Metropolitanas, que são utilizadas quando as distâncias entre os módulos processadores aumenta consideravelmente, atingindo distâncias metropolitanas. Elas podem ser públicas ou privadas.

No exemplo de empresa possuindo diversas fábricas, a rede utilizada permitiria conectar computadores localizados em diferentes prédios numa mesma cidade ou mesmo em cidades distantes de uma dada região. Esta caracteriza uma Rede de Longa Distância ou Rede Geograficamente Distribuída.

Esta classificação não é, de maneira alguma, fechada. Por exemplo, uma rede local pode alcançar dimensões metropolitanas e ainda assim ser considerada local.

A solução para o compartilhamento de recursos físicos e lógicos juntamente com a vantagem de se ter um sistema descentralizado foi alcançada através da interconexão das CPUs entre si. É a isso que se propõem às redes de computadores. A solução para a comunicação de computadores em termos de longa distância foi à tecnologia de comutação de pacotes, que solucionou o problema da linha telefônica dedicada. Para pequenas distâncias a solução foi à implantação de redes locais.

De uma forma geral, o objetivo de uma rede é tornar disponível a qualquer usuário todos os programas, dados e outros recursos independente de suas localizações físicas. Outro objetivo é proporcionar uma maior disponibilidade e confiabilidade, dada a possibilidade de migração para outro equipamento quando a máquina sofre alguma falha. O uso de uma rede de computadores proporciona um meio de comunicação poderoso devido a sua velocidade e confiabilidade.

1.3 Classificação das Redes de Computadores

Uma rede de computadores é formada por um conjunto de módulos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de

comunicação. O sistema de comunicação vai se constituir de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos, através dos meios de transmissão, e de um conjunto de regras com fim de organizar a comunicação, os protocolos de comunicação.

1.3.1 Redes Locais

Redes Locais (LANs - *Local Area Networks*) são redes privadas contidas em um prédio ou campus universitário, que tem alguns quilômetros de extensão. As redes locais foram definidas e utilizadas inicialmente nos ambientes de institutos de pesquisa e universidades. Elas surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

São amplamente utilizadas para interconectar computadores pessoais e estações de trabalho em escritórios e instalações industriais. Nas redes locais as distâncias entre os módulos processadores se enquadram na faixa de alguns metros a alguns poucos quilômetros. Esta definição é bastante vaga, embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias.

As redes locais têm três características que as diferem das demais: tamanho, tecnologia de transmissão e topologia. Elas geralmente tem um tamanho restrito. Em algumas topologias o pior tempo de transmissão é conhecido e isto permite a utilização de determinados tipos de aplicações.

Nas LANs tradicionais os computadores são interconectados por cabos ou através de equipamentos tipo *hub*. Neste tipo de rede as velocidades geralmente variam de 10 a 100 Mbps, há um baixo retardo e pouquíssimos erros de transmissão são encontrados. As LANs mais modernas podem operar em velocidades ainda mais altas, alcançando Gbps.

Este tipo de rede apresenta como topologias lógicas mais usadas o barramento e o anel e como topologias físicas à árvore e a estrela. É fato que em qualquer tipo de rede duas ou mais estações podem necessitar enviar informações pelo meio de transmissão no mesmo instante. Analisando estes arranjos topológicos verificamos que há a necessidade de um mecanismo de arbitragem para determinação de qual estação poderá transmitir de forma a não existência de conflitos e garantia de tempo para todas as estações que têm dados a transmitir.

1.3.2 Redes Metropolitanas

Uma Rede Metropolitana (MAN - *Metropolitan Area Network*) é, na verdade, uma versão ampliada de uma LAN, pois basicamente os dois tipos de rede utilizam tecnologias semelhantes. Uma MAN pode abranger um grupo de escritórios vizinhos ou uma cidade inteira e pode ser privada ou pública. Este tipo de rede pode transportar voz e dados, podendo inclusive ser associado à rede de televisão a cabo local.

A principal razão para se tratar às redes metropolitanas como uma categoria especial é que elas têm um padrão especial, o DQDB (*Distributed Queue Dual Bus*) ou IEEE 802.6. Atualmente as redes ATM (*Asynchronous Transfer Mode*) têm sido a tecnologia com maior aceitação para uso em redes metropolitanas.

1.3.3 Redes Geograficamente Distribuídas

As Redes Geograficamente Distribuídas (WANs - *Wide Area Networks*), ou Redes de Longa Distância abrangem uma ampla área geográfica, com freqüência um país ou continente. Ela também contém um conjunto de máquinas cuja finalidade é executar programas de usuários, as chamadas aplicações. Estas máquinas são denominadas na literatura como *hosts* ou *end systems*. Estes *hosts* são conectados por uma sub-rede de comunicação, ou somente sub-rede. A tarefa as sub-rede é transportar mensagens de um *host* para outro, exatamente como o sistema telefônico transporta palavras da pessoa que fala para aquela que ouve. Esta estrutura é altamente simplificada pois separa os aspectos de comunicação pertencentes à rede (a sub-rede) dos aspectos de comunicação.

Na maioria das redes geograficamente distribuídas, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão, também chamadas circuitos, canais ou troncos, transportam os *bits* entre as máquinas. Os elementos de comutação são equipamentos especializados usados para conectar duas ou mais linhas de transmissão. Quando os dados chegam por uma linha de entrada, o elemento de comutação deve escolher uma linha de saída para encaminhá-la. Não existe uma terminologia padrão para identificar estes equipamentos.

Dependendo das circunstâncias eles são chamados nós de comutação de pacotes, sistemas intermediários, centrais de comutação de dados ou ainda IMP (*Interface Message Processor*). Mas o termo mais comum para identificar estes elementos de comutação é roteador. No modelo mostrado na figura 1.5, os *hosts* são ligados a algum tipo de rede local onde há também um elemento de comutação, embora em alguns casos um *host* possa estar

ligado diretamente a um elemento de comutação. O conjunto de linhas de comunicação e elementos de comutação forma a sub-rede.

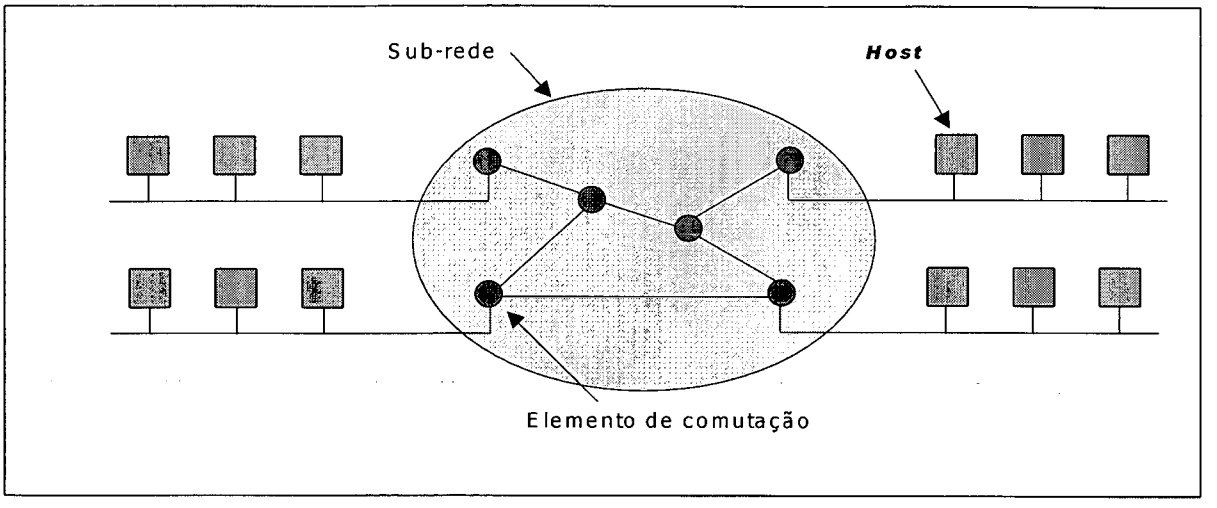

Figura 1.5 - Ligações entre *hosts* e a sub-rede de comunicação

Na maior parte das WANs, a rede contém numerosos cabos ou linhas telefônicas, todos conectados por um par de roteadores. Porém, se dois roteadores que não compartilham um cabo desejarem se comunicar eles poderão faze-lo através de um ou mais roteadores intermediários. Quando um pacote é enviado de um roteador para outro ele é recebido integralmente, armazenado e repassado pela linha de saída quando ela estiver liberada.

Em função dos custos de comunicação serem bastante altos estas redes são, em geral, públicas, isto é, o sistema de comunicação, chamado sub-rede de comunicação, é mantido, gerenciado e de propriedade pública. Também em função dos custos, as velocidades empregadas são relativamente baixas, de alguns *kilobits*/segundo, podendo chegar a *megabits*/segundo.

1.3.4 Redes Sem Fio

As Redes Sem Fio ou *Wireless Networks*, constituem um segmento de mercado que vem crescendo muito. Elas são necessárias quando é impossível haver uma conexão por fios, como por exemplo, a partir de carros ou aviões. Outro problema que elas solucionam é quando uma pessoa viaja e quer usar seu computador portátil para enviar e receber mensagens de correio eletrônico, fax, ler arquivos remotos, estabelecer *login* com computadores remotos, estejam eles em terra, no mar ou no ar. As redes sem fio são muito utilizadas por empresas de caminhões, táxis e por funcionários de assistência técnica ou de vendas, pois estes estão sempre necessitando de informações atualizadas de bases de dados de suas empresas. Elas também têm sido muito utilizadas para operações de resgate em caso de catástrofes onde o sistema telefônico foi destruído e em operações militares.

Embora as redes sem fio e a computação móvel tenham uma estreita relação, elas não são iguais. Às vezes os computadores portáteis podem ser conectados por fios. Por exemplo, se uma pessoa conecta um computador portátil na tomada do telefone de um hotel temos mobilidade sem o uso de uma rede sem fio. Por outro lado alguns computadores com comunicação sem fio não são portáteis. Esse é o caso das empresas sediadas em prédios muito antigos nos quais não há possibilidade de passagem de cabeamento de rede. por vezes a instalação de uma rede sem fio pode ser mais barata do que instalar fiação necessária no prédio.

As redes sem fios são fáceis de instalar mas elas possuem algumas desvantagens: baixa velocidade e altas taxas de erro. Elas também possuem inúmeros formatos. Elas podem variar desde LANs sem fio que cobrem um campus universitário, para que os alunos possam

usar seus computadores portáteis e trabalhar sob a sombra de uma árvore, até o uso de telefones celulares para acesso remoto a redes.

1.3.5 Ligação entre Redes

Existem muitas redes no mundo, freqüentemente com hardwares e softwares específicos. Normalmente as pessoas conectadas a diferentes redes precisam comunicar-se e para que isto seja possível são necessárias conexões entre redes que muitas vezes são incompatíveis. Para que esta comunicação possa realizar-se são utilizados os chamados *gateways*, que estabelecem conexões e permitem a comunicação entre usuários de redes diferentes. Um conjunto de redes interconectadas é chamado de ligação inter-rede, ou apenas inter-rede.

A palavra inter-rede deve ser usada de modo genérico, já a Internet é uma inter-rede mundial específica, muito utilizada para interconectar universidades, órgãos do governo, empresas e pessoas físicas.

As sub-redes, redes e inter-redes são freqüentemente confundidas. Uma sub-rede faz mais sentido no contexto de uma rede geograficamente distribuída, onde fazem referência ao conjunto de roteadores e linhas de transmissão do operador da rede. Por outro lado, a combinação de uma sub-rede e seus *hosts* forma uma rede. Uma inter-rede é formada quando diferentes redes são conectadas.

1.4 As arquiteturas de rede

Em 1972 entrou em funcionamento o projeto piloto da rede ARPA (*Advanced Research Project Agency*). Começava ai a era da tecnologia de redes de computadores, caracterizada pela distribuição das aplicações entre vários comutadores interligados de acordo com uma topologia determinada. Na rede ARPA foi, pela primeira vez, implementada a tecnologia de comutação de pacotes, assim como o método de divisão em várias camadas funcionais das tarefas de comunicação entre aplicações residentes em computadores distintos, conectados por meio da rede, criando-se o conceito de Arquitetura de Rede de Computadores. Também na década de 70, o crescimento da ARPA permitiu a interligação de computadores de universidades americanas e de alguns computadores situados em outros países.

Na mesma época, os grandes fabricantes de equipamentos de processamento de dados criaram seus próprios métodos para interligar em rede seus respectivos produtos. Surgiram, assim, as Arquiteturas Proprietárias, primeiro com a IBM, que lanços a arquitetura SNA (*Systems Network Architecture*), depois com a Digital e a sua arquitetura Decnet, além de várias outras.

Para as entidades especializadas em venda de serviços de telecomunicações abriu-se um novo mercado: a oferta de serviços de comunicação de dados por meio do fornecimento de uma estrutura de comunicação, a sub-rede, baseada funcionalmente no princípio de comutação de pacotes. O CCITT (atual ITU-T) elaborou documentos que permitiram que estes serviços fossem padronizados, a partir dos quais publicou, em 1976, a primeira versão da Recomendação X.25, propondo a padronização de redes públicas de comutação de pacotes.

1.5 A arquitetura do RM/OSI

O quadro que o segmento de redes de computadores apresentava no final da década de 70 caracterizava-se, de um lado, por enormes perspectivas de crescimento, mas, de outro, por uma situação de crise criada pela heterogeneidade dos padrões, protocolos e equipamentos de comunicação de dados existentes no mercado. Cada interessado havia definido, unilateralmente, sua arquitetura. Os fabricantes, as arquiteturas proprietárias; as operadoras de telecomunicações, as arquiteturas das redes públicas; e algumas entidades, como era o caso da ARPA, arquiteturas específicas para atender às suas redes.

A solução foi encontrada pela ISO (*International Organization for Standardization*), sob a forma de propostas de elaboração de um modelo que viesse a sintetizar, de modo abstrato, o funcionamento de computadores integrados por redes de comunicação de dados. Baseada nas experiências advindas do funcionamento dos sistemas de teleprocessamento, da rede ARPA e das redes públicas e proprietárias, a ISO, entre 1978 e 1984, elaborou o RM-OSI ou Modelo de Referência para Interconexão de Sistemas Abertos (*Reference Model - Open Systems Interconnection*), que é a expressão, assim, de todo o conhecimento tecnológico adquirido pelo mundo a respeito de comunicação de dados.

No modelo OSI foi, pela primeira vez, abordado o conceito de sistema aberto, definido como "o sistema capaz de suportar os padrões de comunicação OSI de modo a interfuncionar com outros sistemas abertos de diferentes fornecedores". Ao modelo OSI se deve, também, a consolidação dos princípios de arquitetura de rede de comunicação de dados.

O esforço de padronização não foi concluído com a elaboração do Modelo OSI. Ao contrário, iniciou-se uma intensa atividade, em nível mundial, no sentido de projetar, especificar, implementar e testar os protocolos das várias camadas definidas pelo modelo,

nascendo, assim, a Arquitetura OSI: uma estrutura funcional dos elementos envolvidos na comunicação entre sistemas abertos de comunicação de dados, suportada por um conjunto de protocolos padronizados, elaborados de acordo com os princípios do Modelo OSI.

Desde a sua criação, e cada vez que um novo padrão de protocolo é elaborado, a Arquitetura OSI impõe-se como o grande projeto de Engenharia de Protocolos. As soluções apresentadas, os mecanismos de protocolos, a estrutura de camada de aplicação e as aplicações desenvolvidas de acordo com os princípios da metodologia orientada a objetos e da computação distribuída contribuem para essa colocação.

1.6 A Arquitetura TCP/IP – Internet

A arquitetura Internet é largamente utilizada para interconexão e interoperação de sistemas computacionais heterogêneos. Tal arquitetura foi lançada pelo Departamento de Defesa do governo americano e escolhida para ser o padrão obrigatório de comunicação entre os diversos sistemas daquela organização. Ela tornou-se um padrão *de fato* do mercado. Os padrões não são definidos por entidades de padronização internacional como a ISO, por exemplo. As definições dos protocolos são encontradas em documentos denominados RFC (*Request for Comments*), os quais são elaborados pelo IAB (*Internet Activities Board*).

A arquitetura Internet também é organizada em camadas. Ela é composta por dois protocolos principais: o IP (*Internet Protocol*) e o TCP (*Transmission Control Protocol*). O IP é responsável pelo encaminhamento de pacotes de dados pelas diversas sub-redes desde a origem até o seu destino. O TCP tem por função o transporte fim-a-fim confiável de

mensagens de dados entre dois sistemas. O IP é um protocolo do tipo datagrama, operando, portanto, no modo não orientado à conexão, enquanto o TCP é um protocolo de transporte orientado à conexão. O conjunto TCP/IP pode, desta forma, oferecer um serviço relativamente confiável. Para uso em redes de alta qualidade, onde o problema de confiabilidade não assume grande importância, foi definido o protocolo UDP (*User Datagram Protocol*) que opera no modo não orientado à conexão e possui funcionalidades bem mais simplificadas que o TCP.

1.7 As Redes Locais

Geralmente uma rede local serve a uma área geograficamente limitada, isto é, um ambiente de trabalho, um edifício, um campus universitário, uma fábrica, etc. As distâncias podem variar de metros até alguns poucos quilômetros e a velocidade de transmissão é da ordem de milhões de *bits* por segundo. A maioria dos produtos existentes na área utiliza uma forma simples de interligação física entre os equipamentos e talvez esta seja uma das características mais atrativas das redes locais.

Estas características, no entanto, não são suficientes para garantir o sucesso de uma rede local. Para o usuário final é muito importante ter um mecanismo de transmissão de informação eficiente, sem que haja a necessidade de conhecer os detalhes técnicos para efetuar a ligação com a rede.

Uma rede local pode ser descrita através de características tais como: está contida dentro de uma área geográfica limitada, possui equipamentos interconectados porém independentes, existe um alto grau de interconexão entre os equipamentos da rede, a transmissão de informação é geralmente na forma digital, a interface com a rede é feita

através de equipamentos e meios de transmissão relativamente baratos e é possível a comunicação entre dois equipamentos quaisquer da rede.

A escolha de um tipo de rede para suporte a um dado conjunto de aplicações é uma tarefa por vezes difícil. Cada arquitetura de rede possui características que afetam sua adequação a uma aplicação em particular. Muitos podem ser os atributos que fazem parte do rol possível de ser considerado para comparação. Dentre eles estão: custo, tempo de resposta, velocidade, desempenho, confiabilidade, modularidade, compatibilidade, e facilidade de adaptação na mudança de tecnologia.

1.7.1 O RM-OSI e as redes locais

Redes locais possuem características que afetam principalmente os níveis mais baixos de protocolo de uma arquitetura de rede. Esses níveis não devem deixar de levar em consideração o elevado desempenho, o baixo retardo, a baixa taxa de erros, o roteamento simples (em geral único) e as aplicações a que se destinam as redes locais.

O RM-OSI, embora teoricamente, poderia ser utilizado tanto em redes geograficamente distribuídas como em redes locais. No entanto, ele foi pensado para uso em redes geograficamente distribuídas. Sua aplicabilidade em redes locais não pode deixar de levar em consideração as características intrínsecas destas redes.

As distâncias limitadas a que são destinadas as redes locais permitem que seu protocolo de nível físico possa utilizar um meio de alta velocidade com baixíssimas taxas de erros. Este fato vai influenciar em muito os outros níveis de protocolo.

Várias diferenças existem na camada de enlace de dados, a começar pela delimitação dos quadros. Ao contrário das redes de longa distância, nas redes locais o método mais apropriado para delimitação de quadro pode ser a simples presença ou ausência de sinal no meio.

1.7.2 Interconexão de redes locais

A interconexão de redes locais é uma necessidade nos dias atuais. Esta é a tarefa mais importante da camada de rede em redes locais. Ela se faz necessária quando máquinas origem e destino estão em redes diferentes. Na execução da função de ligar rede locais entre si pode-se criar topologias parcialmente ligadas fazendo com que existam caminhos diferentes por redes intermediárias, com diferentes protocolos. O principal problema que decorre disto é que existem diversos tipos de redes com características próprias. Assim, a tarefa do nível de rede é compatibilizar as diferentes tecnologias e protocolos empregados nas redes a serem interconectadas.

Nem sempre a interconexão de redes exige alto grau de complexidade. Por vezes é apenas necessário ligar dois segmentos de rede exatamente iguais, ou que possuam apenas o meio físico diferente. Por exemplo quando desejamos interconectar duas redes Ethernet somente com cabeamento diferente. Outro problema, um pouco mais complexo, seria interconectar duas redes com protocolos de acesso diferentes, porém com o mesmo protocolo de rede. Por exemplo, se desejarmos interconectar uma rede Ethernet com uma rede *Token Ring*.

As motivações que podem levar à necessidade de interconectar de redes entre si são:

de ordem econômica, por exemplo, para compartilhar uma interface de rede pública;

de ordem tecnológica, por exemplo, para interconectar várias redes locais em áreas ou prédios distintos;

para melhorar desempenho e confiabilidade, por exemplo, dividir uma rede local com grande número de estações em 2 ou mais redes;

de ordem funcional, por exemplo, para atender necessidades do usuário, tais como acesso a recursos como bancos de dados, disponíveis em outras redes.

Algumas questões a serem abordadas para a interconexão:

endereçamento e encaminhamento das mensagens;

fragmentação das mensagens;

detecção e recuperação de erros;

serviço com ou sem conexão;

nível de interconexão;

controle de fluxo;

controle de congestionamento;

segurança;

tarifação de serviços;

nomes e endereçamento.

A ligação entre equipamentos heterogêneos deve ter convenções para representação de nomes e endereços de processos que tenham significado em toda a rede. As referências às redes são feitas por nomes ou por endereços, e isto é importante para identificação de recursos na rede. A maneira mais comum é o endereçamento hierárquico, ou seja, o endereço do processo constituído de endereço da rede, endereço do equipamento hospedeiro (*host*) e endereço dentro do hospedeiro (porta). Há também uma alternativa, o endereçamento plano, ou não-hierárquico, onde há um endereço para cada recurso na rede.

É importante lembrar que a interconexão de duas redes exige a implementação, em cada rede, de um protocolo inter-redes que realize, pelo menos, as funções de tratamento de endereços. Os principais equipamentos para interconexão de redes são: repetidores, pontes (bridges) e roteadores.

2 Segurança

2.2 A Importância da Informação na Empresa

Para administrar os negócios e tomas decisões, os administradores da empresa apoiam-se em diversas informações contábeis, administrativas. Assim sendo, a informação é essência das atividades e negócios da empresa. É o bem mais precioso da empresa, depois da vida humana. A empresa depende das informações.

É imprescindível, portanto, que as informações sejam suficientes, exatas, disponíveis a tempo e suficientemente protegidas.

2.3 A Importância da Tecnologia na Empresa

A maioria das informações de uma empresa é normalmente concentrada e processada em computadores. Bens, pessoas e serviços são controlados por sistemas de informação processados pelo(s) computador(es).

A tecnologia funciona como o "coração" da empresa. A empresa depende dos computadores. Deficiências, erros, omissões, falhas, irregularidades, acidentes e desastres no ambiente do computador podem afetar seriamente as atividades, operações e negócios da empresa.

Uma paralisação prolongada no processamento de informações, ocasionada por uma acidente ou desastre, pode gerar sérios prejuízos e comprometer a empresa. A sobrevivência de uma empresa depende da sua capacidade de processar informações.

Uma paralisação prolongada no processamento de informações essenciais pode ocasionar danos a empresa:

declínio de atividades, operações e negócios;

insatisfação dos clientes não atendidos;

queda nas vendas/faturamento;

perda de reputação;

sanções legais;

sérias dificuldades para se recuperar;

falência da empresa;

Como ilustração, apresentamos a seguir algumas conclusões baseadas em estatísticas dos Estados Unidos da América.

"A probabilidade que tem uma empresa de médio ou grande porte de sofrer um desastre que afete o seu CPD é de 1 em 100. A probabilidade de sobreviver a esse desastre é de 7 em 100".

"Uma empresa de médio ou grande porte perderá de 2 a 3 % de suas vendas brutas dentro de 8 dias de paralisação de seus recursos computacionais".

"Uma paralisação de processamento de dados, durante meio-dia, numa instituição financeira, resultará numa perda de 13% da atividade normal da empresa. Uma paralisação durante 10 dias resultará numa perda de 97% da atividade normal da empresa".

"Uma empresa de médio ou grande porte que sofrer uma paralisação de seus recursos computacionais por mais de 10 dias, dificilmente se recuperará totalmente. Provavelmente este empresa estará fora de atividade dentro de 5 anos".

A problemática causada pela paralisação prolongada no processamento das informações essenciais, no CPD ou em algum departamento usuário, atinge instâncias onde se torna difícil a quantificação dos prejuízos e conseqüências. Dentro das funções da empresa, destacamos com críticas as seguintes: faturamento; PCP; Folha de Pagamento; Contas a Receber/Pagar, etc.

2.4 Estratégias de Segurança

Segurança geralmente envolve o uso de várias estratégias para sua implementação, como por exemplo: Menor privilégio, Defesa em profundidade, Ponto de controle, Elo mais fraco, Falhar com segurança, Participação universal e Simplicidade

Menor privilégio

Qualquer agente só deve ter o mínimo de privilégio suficiente para desempenhar suas tarefas, como abaixo exemplificado:

Nunca fornecer a um usuário uma senha privilegiada para fazer apenas uma operação: criar um perfil específico.

Nunca deixar seus sistemas internos confiar nos firewalls, por exemplo, para usar uma fita (remota) para cópias de segurança.

Defesa em profundidade

O uso múltiplos mecanismos redundantes, em caso de falhas ou comprometimento de um dos mecanismos, ainda haverá alguma proteção.

Ponto de controle

Obriga os atacantes a usar um canal estreito, fácil de monitorar e controlar, evitar permitir caminhos alternativas a sua rede que não passem por controles, p.ex. acesso discado.

Elo mais fraco

A qualidade de uma defesa depende no seu elo mais fraco, é preciso conhecer os diferentes pontos vulneráveis e concentra os esforços nos mais fracos. Segurança de hosts se complica pelo fato que não existe um único ponto de controle: cada serviço fornece uma entrada separada ao sistema

Falhar com segurança

Em caso de falha, as defesas devem manter a ameaça *excluída* , ao invés de admiti-la. A postura geral em respeito à segurança podem ser:

Postura repressiva: Proíbe-se tudo que não é expressamente permitido. Examinando os serviços desejados pelos usuários e considerando as implicações de segurança de cada um, e como podem ser atendidos, permite-se apenas os serviços que se entende, pode prover com segurança, e são justificáveis. Exemplos: um serviço pode ser implementado com segurança e

será liberado para todos os usuários; outro, difícil de segurar, só seria liberado para alguns usuários específicos e adequadamente treinados.

Postura permissiva: Permite-se tudo que não é expressamente proibido. Inicialmente tudo é permitido, depois se inicia o corte de serviços considerados inseguros: NFS não será permitido através do Firewall; acesso WWW limitado a usuários treinados em problemas de segurança, é proibida a criação de um servidor por um usuário comum.

Participação universal

Sem a cooperação dos seus usuários é difícil garantir a segurança, exemplos: acessos paralelos à sua rede, via ligações discadas; esquemas de promover modificação de senhas reutilizáveis podem hostilizar os usuários.

Simplicidade

Torna as coisas (software, políticas) mais fáceis de entender, sem compreender um sistema, não podemos afirmar que é seguro. Todo software complexo tende a ter mais "bugs", inclusive que comprometem a segurança do sistema. Basicamente, o princípio KISS (Keep It Simple, Stupid).

2.5 Segurança Redes de Computadores (Sistemas Distribuídos)

A segurança efetiva dos recursos computacionais de uma empresa é uma necessidade essencial porque envolve não apenas instalações físicas e equipamentos, mas também interesses dos usuários, executivos, acionistas, clientes e da comunidade. Portanto, a

segurança é, antes de tudo, uma preocupação administrativa e não técnica. Segurança é investimento e não despesa.

Funções de Segurança

As funções básicas das medidas de segurança são:

Discussão (desencorajamento à prática de irregularidades); prevenção (redução da ocorrência de riscos); detecção (sinalização da ocorrência de riscos); contenção (limitação dos impactos dos riscos); recuperação (alternativas para a continuidade operacional); restauração (correção dos danos causados pelos riscos).

Uma segurança efetiva envolve a implementação simultânea de suficientes medidas que suportam todas as funções acima.

Tipos de Segurança

Os tipos de segurança (ou linhas de defesa) são: segurança física: abrange medidas de proteção relacionadas à localização e construção do CPD, acesso físico, instalações elétricas, fogo, água, condições ambientais, pessoal, equipamentos, etc; segurança lógica: abrange medidas de proteção relacionadas a sistemas/programas, dados/informações e documentação; segurança administrativa: abrange políticas, diretrizes, normas e procedimentos de segurança.

Objetivos de Segurança de Computadores

As medidas de segurança no ambiente de computadores visam: garantir a integridade dos bens e serviços da empresa que estão sob o controle dos sistemas de informação processados pelo computador; garantir a exatidão, confidencialidade, disponibilidade e proteção das informações concentradas e processadas no computador; garantir a proteção dos

recursos (materiais, humanos, financeiros e tecnológicos) no ambiente de computadores; garantir a continuidade (disponibilidade) da capacidade de processamento de dados; garantir funções, responsabilidades, operações e procedimentos são executados conforme instruções em vigor.

Implementação da Segurança

A implementação de segurança no ambiente de computadores envolve as seguintes etapas: designação de uma equipe específica responsável pela segurança de informática; levantamento de todo o ambiente de informática na empresa; realização de uma campanha de conscientização sobre riscos e segurança no ambiente de computadores; realização de uma "Análise de Risco"; determinação de quanto gastar em segurança; determinação de objetivos e prioridades de segurança; elaboração e implementação de um "Plano de Segurança" e de um "Plano de Contingência"; divulgação, testes, atualizações e treinamento periódicos; monitoração da segurança (controles e auditorias).

Equipe de Segurança

Deve existir uma equipe específica para tratar de todos os aspectos relacionados à segurança da informática. Esta equipe deve estar posicionada em nível de assessoria da gerência do CPD, e não em nível de órgão de linha.

As responsabilidades básicas dessa equipe são: planejamento, implantação e controle das medidas de segurança. Isso inclui a realização de uma "Análise de Risco" e a elaboração e implementação de um "Plano de Segurança" e de um "Plano de Contingência".

Análise de Risco

Uma das primeiras tarefas da equipe responsável pela segurança é a realização de uma "Análise de Risco" que envolve as seguintes etapas básicas: identificação dos bens, pessoas e serviços a serem protegidos; identificação dos tipos de riscos a que se está sujeito cada bem, pessoa ou serviço a ser protegido. Estimativa da probabilidade de ocorrência de cada tipo de riscos no período de um ano; estimativa da perda financeira a cada ocorrência de cada tipo de risco; cálculo da perda financeira anual para cada tipo de risco; cálculo da perda financeira total para todos os riscos; pesquisa e seleção das medidas de segurança necessárias; cálculo do custo de implementação e manutenção das medidas de segurança necessárias; análise custo x benefício (economia anual que poderá ser obtida com a implementação das medidas de segurança).

A realização de uma Análise de Risco proporciona discussões sobre assuntos de segurança e, conseqüentemente, melhoria de conhecimento, preocupação e interesse sobre segurança. Além disso, provê fundamentos para decisões e justificativas para gastos com segurança. A análise de risco é a base para a elaboração de um "Plano de Segurança".

Plano de Segurança

O Plano de Segurança de Informática, como o próprio nome indica, é um documento (manual) específico para cada empresa - que descreve detalhadamente todos os aspectos relacionados à segurança no ambiente de informática: políticas, diretrizes, metas, responsabilidades, providências, normas e procedimentos sobre segurança de computador; medidas de segurança: preventivas (segurança física, segurança lógica) corretivas (Plano de Contingência)

Procedimentos de Contingência

Os procedimentos de contingência (recuperação de desastre) constituem o Plano de Ação (do Plano de Contingência), devem ser definidos (no Plano de Contingência) para orientar as pessoas e departamentos da empresa sobre suas responsabilidades e ações no caso de um desastre, e, devem definir "quem" faz o "que", "onde", "quando", e "como", numa situação de desastre;

A apresentação deve ser de forma simples e clara (o uso de desenhos, gráficos, figuras, ajuda muito). Suficientes cópias desses procedimentos (Manual do Plano de Contingência) devem estar prontamente disponíveis no CPD e nos departamentos envolvidos, para o evento de um desastre.

Tipos de Procedimentos de Contingência

Diversos são os tipos de procedimentos de contingência que devem ser definidos no Plano de Contingência. Tais procedimentos são específicos para cada Plano de Contingência. Depende de cada empresa.

Por exemplo:

Classes de procedimento de contingência:

procedimentos de reação inicial de emergência;

procedimentos de recuperação das aplicações críticas na instalação alternativa;

procedimentos de restauração da instalação afetada e volta à situação (processamento) normal.

Procedimentos de reação inicial de emergência (ação imediata):

procedimentos de evacuação, salvamento, abrigo;

procedimentos de notificação, contato das pessoas, departamentos e entidades externas envolvidos no evento de um desastre;

procedimentos de combate, supressão do desastre;

procedimentos de caracterização, declaração de desastre;

procedimentos de ativação do Plano de Contingência;

Procedimentos de recuperação:

procedimentos de acesso e uso de itens guardados no armazenamento remoto;

procedimentos de transferência das operações para a instalação alternativa;

procedimentos de recuperação das comunicações;

procedimentos de operação na instalação alternativa.

Procedimentos de restauração:

procedimentos de restauração física da instalação original acidentada;

procedimentos de restabelecimento das operações na instalação original;

procedimentos de retorno à instalação original.

2.6 Hackers / Crackers / Invasão

O termo Hacker, originalmente, designava qualquer pessoa que fosse extremamente especializada em uma determinada área. Qualquer fera em qualquer assunto, poderia ser considerado um hacker. Somente com a ajuda do cinema americano, é que o termo Hacker de Computador passou a ser utilizado largamente, mas nem por isso perdeu sua identidade.

Seguindo a lógica americana, que produz "filmes propagandas" que induzem os telespectadores a desejarem ser o que o filme mostra - assim como TopGun foi uma propaganda à Marinha, e Cortina de Fogo uma propaganda para o Corpo de Bombeiros, com War Games aconteceu à mesma coisa: vários adolescentes que tinham um modem começaram a sonhar com os controles da terceira guerra mundial em suas mãos, ou mais especificamente em sua escrivaninha, no quarto.

Isso não quer dizer que este filme foi à base de lançamento de atitudes hacker por todo o mundo, mas foi um dos responsáveis pela dilatação desses pensamentos. O mercado americano abarrotou as prateleiras de livros como Cyberpunk, e mais tarde, qualquer nota sobre invasão de sistemas ou crimes relacionados a computadores ganhavam um espaço cada vez maior na mídia. Existiam hackers de verdade sim! Eram pessoas que trabalhavam em projetos de computadores e técnicos altamente especializados. Mas também existiam aqueles garotos, que após descobrirem que invadir um sistema ou lançar um míssil não era tão fácil quanto ver um filme ou ler um livro, insistiram e estudaram muito (as maiores virtudes dos hackers são à força de vontade e a dedicação aos estudos), conseguiram muitas proezas e hoje, grande parte trabalha na área de segurança de computadores. O resto está preso.

A grande maioria dos hackers é jovem. Dizem que é uma fase da vida de cada micreiro. E além do mais o jovem tem muito mais tempo para estudar e aprender. Depois que

cresce, precisa se preocupar com a vida de verdade e passa a trabalhar (geralmente com computadores), deixando de invadir sistemas ou fazer coisas piores. Os poucos que continuam a praticar atos de hacker são espiões industriais ou especialistas em segurança, e passam a fazer um jogo de gente grande, onde a pessoa vai precisar deter de verdade os invasores perigosos (os espiões), e estes se protegerem do risco de invadir sistemas (e da polícia).

Portanto, hackers existem, são e sempre serão poucos! Quando (e se) uma "informação de hacker" chegar às mãos de principiantes, com certeza é porque ela está difundida demais, e não será útil para mais nada.

Conhecemos (de perto) hackers (ou pretendentes a) que passam a noite inteira tentando quebrar um código, conseguir acessos não autorizados, burlar esquemas de segurança e, às vezes, estragar sistemas de computação.

2.6.1 As Motivações do Hacking

Há muito tempo se ouve falar de adolescentes que passam a noite inteira invadindo sistemas de computadores. Entretanto, muito pouco se fala dos mais perigosos hackers. O motivo pelo qual os jovens ganham destaque na mídia é a sua captura, pois eles não possuem conhecimento suficiente para que se mantenham ocultos por muito tempo. Por pura inexperiência, deixam rastros por onde passam, pelo descuido e inconseqüência, ou porque simplesmente não têm motivos para se esconderem.

Do outro lado, estão os hackers profissionais, extremamente cuidadosos com suas investidas, e são muito mais difíceis de se detectar e capturar. Afinal, estes não estão mais brincando.

Independente do tipo de hacker, as motivações para seus ataques são bastante variadas, e podemos dividir suas ações em algumas categorias distintas:

Espionagem Industrial: Pode ocorrer de uma empresa contratar um hacker para que este invada o sistema da concorrência e descubra seus planos, roube seus programas ou até mesmo suas políticas de parcerias e de investimento. (geralmente praticadas por hackers profissionais)

Proveito Próprio: O hacker pode invadir um sistema para roubar dinheiro, transferir bens, cancelar dívidas ou até mesmo ganhar concursos. Qualquer ação em que ele seja diretamente beneficiado.

Inexperiência: Há também o caso de uma invasão ocorrer por ignorância. Por exemplo, um funcionário que acessa sua conta da empresa através do seu micro em casa. Dependendo da política de segurança da empresa, isto pode ser considerado uma invasão, mesmo que o usuário não tenha conhecimento do problema que pode causar.

Vingança: Um ex-funcionário, tendo conhecimento do sistema, pode causar vários problemas, se o gerente de segurança da empresa não "cortar" seu acesso imediatamente após sua saída da empresa. Ou, um parceiro de pesquisas pode acessar "mais do que deve" após a quebra de um contrato, trazendo complicações e prejuízos à empresa.

Status ou Necessidade de Aceitação: Uma invasão difícil pode fazer com que o invasor ganhe um certo status junto aos seus colegas. Isso pode acarretar uma competição, ou

uma verdadeira "gincana" na sua empresa. Dentro de grupos, é constante a necessidade de mostrar sua superioridade. Este é um fato natural, seja entre humanos, animais selvagens ou hackers.

Curiosidade e Aprendizado: Muitos hackers alegam invadir sistemas apenas para aprender como eles funcionam. Alguns fazem questão de testar o esquema de segurança, buscando brechas e aprendendo sobre novos mecanismos. Este tipo de ataque raramente causa um dano maior ou compromete os serviços atacados.

Busca de Aventuras: O ataque a sistemas importantes, onde os esquemas de segurança são muito avançados, podem fazer com que o hacker se sinta motivado pelo desafio e pelo perigo de ser pego, assim como alpinistas sobem montanhas, mesmo sabendo do risco de caírem.

Maldade: Algumas pessoas sentem prazer na destruição. Invadem e destroem, pelo puro prazer de causar o mal. Raramente são pegos e se vangloriam dos seu atos.

2.6.2 Os Pontos Fracos

Existem inúmeras categorias de ataque a serviços Internet, explorando falhas de software, hardware e principalmente burlando esquemas de segurança ineficazes em nossas políticas operacionais. Por exemplo:

Sniffer: Captura informações que trafegam pela rede, como logins e senhas em texto não-criptografado, podendo ser utilizadas futuramente por um invasor.

Spoof: Baseia-se na confiança da negociação entre servidores, que acreditam na veracidade do endereço de origem daquela ordem ou informação, e podem sofrer um ataque por mensagens na qual a origem é "disfarçada" como sendo de alguém de confiança.

Mudanças de rota: Um ataque desta natureza pode fazer com que toda a informação de um dado servidor seja obrigada a passar por um espião antes de seguir seu caminho, ou simplesmente sejam redirecionadas para lugar nenhum, causando a "queda" do serviço.

Trojan Horse: Um programa pode ser inadvertidamente instalado em um servidor, o qual permitiria uma invasão por alguma porta ou "brecha" propositadamente implantada neste programa.

Replay: Alguma ação, comandos ou seqüência de eventos podem ser observados durante um processo de autenticação, e repetidas, posteriormente, por um invasor para obter acesso a estes sistemas.

Vírus: À primeira vista pode parecer um simples problema de usuários domésticos, mas os vírus, se não forem devidamente eliminados e controlados, podem causar, direta e indiretamente, vários problemas em uma rede, desde a impossibilidade de comunicação interna, até a interrupção dos serviços vitais.

Adulteração: A falta de um controle de conteúdo eficiente pode fazer com que uma informação seja adulterada durante sua transmissão, pondo em risco a comunicação entre dois sistemas.

Alguns produtos, tais como servidores ou até mesmo sistemas operacionais completos, vêm configurados "da fábrica" de uma forma muito pouco segura, e é necessário conhecer

todos os aspectos da nova ferramenta instalada no seu sistema para que ela seja corretamente utilizada.

Programas como servidores de mail, ftp, web ou configurações do sistema, como permissões de arquivos, aplicativos desnecessários (tal como um lpd em um servidor exclusivo de web) devem ser completamente vistoriados antes da sua instalação, procurando se informar sobre suas capacidades de auditoria e sobre seus recursos de segurança.

Pode-se ainda, caso o sistema em questão seja inseguro e necessário, cogitar produtos que possam implementar esta segurança à parte, e dar a mesma importância a eles, instalando-os simultaneamente, e nunca "deixar para depois", pois se alguém detectar uma falha no seu sistema, ela será explorada imediatamente!

E o mais importante: estas configurações padrões, ou os erros mais comuns durante as instalações, são os primeiros alvos dos hackers e, em pouquíssimo tempo seu sistema poderá ser completamente comprometido por pura falta de atenção.

2.6.3 As Ameaças do Hacking

O simples fato de estar conectado à Internet implica em uma série de possibilidades de atentado à sua segurança. Entre as principais ameaças estão:

Redes Corporativas: Disponibilizar serviços Internet em uma rede corporativa pode abrir diversos furos de segurança, permitindo que recursos ou informações da empresa sejam acessados de forma indevida por estranhos.

Servidores: A ameaça de alteração nas informações de servidores pode ser mortalmente prejudicial para uma empresa. Por exemplo, a modificação da especificação de algum produto em um servidor da web pode fazer com que inúmeros negócios sejam perdidos.

Transmissão: Às vezes pode não ser necessário uma invasão de servidores ou redes. É possível violar a transmissão da informação pela Internet, interceptando-se mensagens, arquivos, senhas etc.

Interrupção: Um serviço pode ser atacado de uma maneira menos sutil, mas nem por isso menos perigosa. Pode-se, simplesmente, fazer com que o serviço "caia", deixe de funcionar, e que todos os seus usuários legítimos fiquem inacessíveis.

Negação: Em transações pela Internet, ainda temos um outro problema a solucionar. Negar a participação em uma negociação digital também pode ser considerada um ataque ao seu correto funcionamento.

2.7 Ferramentas de Segurança

2.7.1 Criptografia

A criptografia é uma arte: a arte de escrever ocultamente. Talvez tão antiga quanto à própria escrita, hoje é um dos métodos mais eficientes de se transferir informações, sem que haja a possibilidade de comprometimento do sigilo.

Baseada em chaves, uma informação pode ser codificada através de algum algoritimo de criptografia, de modo que, tendo conhecimento do algoritimo utilizado e da chave utilizada, é possível recuperar a informação original fazendo o percurso contrário da encriptação, a decriptação.

Com o aumento da capacidade computacional, podemos hoje utilizar complexos esquemas criptográficos, que antes eram impraticáveis pela demora com os quais eram codificadas pequenas informações. E além da capacidade técnica, possuímos algumas características na criptografia moderna que a faz se subdividir em dois grandes grupos: Criptografia de Chave Simétrica e Criptografia de Chave Assimétrica.

Criptografia de Chave Simétrica

Esta é a criptografia tradicional, onde a mesma chave utilizada na codificação deve ser utilizada da decodificação. Alguns algoritimos de criptografia de chave simétrica: IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard) da IBM e o RC2/4, da RSA Data Security.

No entanto, a criptografia simétrica é bastante eficiente em conexões seguras na Internet, onde processos computacionais trocam senhas temporárias para algumas transmissões críticas. Quando se navega pela Internet e visita-se os sites ditos "seguros", onde geralmente são preenchidos dados sigilosos, está utilizando-se o SSL (Secure Sockets Layer) que funciona à base de criptografia simétrica, muito provavelmente um DES ou algo da RSA.

Criptografia de Chave Assimétrica

Estudos realizados há uns 20 anos tornaram possíveis algoritimos de criptografia utilizando duas chaves. Criptografando-se com a chave A, só seria possível a decriptação com a chave B, sendo a recíproca verdadeira!

Chave Pública e Chave Privada

Esta assimetria nos dá uma outra abordagem: a de chave pública e chave privada. Com duas chaves, não precisamos ficar presos a uma "troca" para o processo de decodificação / codificação. Cada um poderá possuir chave pública e chave privada. Como o próprio nome já diz, a chave privada é de conhecimento único e exclusivo. Já a pública deve estar disponível a quem quiser lhe enviar informações encriptadas.

Como a encriptação/decriptação depende das duas chaves, para, por exemplo, enviar uma mensagem criptografada, deve-se encriptá-la com a chave pública. A única chave que decripta esta mensagem é o par da chave pública, ou seja, a chave privada. Somente o proprietário conseguirá ler a mensagem.

Uma mensagem comum, em texto simples, pode ser lida em qualquer local da Internet, em especial no provedor de acesso, ou na conta do mail gratuito ou algo do gênero. Apesar da política na maioria dos serviços proibir a leitura de mensagem dos usuários, ela é totalmente possível.

Assinatura Digital

A criptografia por chaves assimétricas vale para ambos os lados: Pública » Privada e Privada » Pública. Encriptando uma mensagem com a chave PRIVADA, qual é a única chave capaz de decriptá-la? "a chave PÚBLICA". Aparentemente não é muita vantagem, pois todos

têm acesso à chave pública e poderão ler a mensagem ? Realmente, todos os que possuírem a chave pública poderão ler a mensagem, mas também é verdadeiro que, se foi possível decriptar com a chave pública, é porque ela foi encriptada com a chave privada! Como a única pessoa que sabe a chave privada é o seu criador, está assegurada a identidade do autor daquela mensagem.

Simétrica, Assimétrica

Há um pequeno problema na criptografia com chave assimétrica: ela é muito lenta! É preciso um computador com grande capacidade de processamento para que o tempo de criptografia se torne viável, pois um texto grande pode levar de alguns minutos a várias horas. Já a simétrica... Ela é rápida, mas possui o problema da chave única.

Existe uma maneira de se criar um código a partir de uma mensagem, que reflita o seu conteúdo em um pequeno conjunto de caracteres. Aplica-se um cálculo na mensagem e o seu resultado passa ser um "message digest", como se fosse uma impressão digital da mensagem. Uma letrinha trocada e o message digest será diferente.

Alguns algoritimos que fazem a "extração" do message digest mais utilizados no mercado: MD4/5 e o SHA (Secure Hash Algorithm).

O cálculo do message digest possui duas características fundamentais: não pode ser possível inverter o cálculo sobre o message digest para recuperar a mensagem original; e o message digest deve ser único por mensagem, ou seja, não pode existir um mesmo message digest para duas mensagens diferentes.

Com essa nova ferramenta, pode-se assegurar a autenticidade com criptografia assimétrica, mas nos poupando tempo.

2.7.2 Firewalls

Uma das grandes preocupações na área de segurança de redes é a vulnerabilidade de um computador, que pode comprometer as transmissões pelo meio físico da rede na qual está ligado. Muito se tem feito para que o host (equipamento computacional) esteja seguro isoladamente, impedindo o acesso indevido a seus dados e monitorando qualquer tentativa de invasão. Entretanto, um outro método tem se mostrado bastante eficiente: impedir que informações indesejadas entrem na rede como um todo.

Não é um método substituto à Segurança do host, mas complementar, e consiste no seguinte: na ligação da rede interna com a Internet, instala-se um equipamento que permitirá, ou não, a entrada e saída de informação, baseado em uma lista de restrições e permissões, devidamente configurada para suprir as necessidades básicas de comunicação da rede interna com a Internet e vice-versa. Nem mais, nem menos. Esta configuração é a chave do sucesso ou fracasso de um firewall.

É importante lembrar que o firewall deve estar presente em todas as conexões da rede interna com a Internet. Não adianta nada colocar um firewall super sofisticado na ligação do backbone se, dentro da rede interna, existir um micro com um modem conectado em outra rede.

A Filtragem de Pacotes

Essa é a maneira mais simples de se construir um firewall. Geralmente utilizadas em roteadores, as listas de acesso têm uma ótima relação custo x benefício: os roteadores já possuem estas facilidades, basta sentar e aprender a configurá-los; a filtragem é bem eficiente, invisível e rápida.

Os roteadores têm um papel muito simples: interligam duas redes e fazem o transporte de pacotes de informação de uma rede para outra, conforme sua necessidade. Mas muitos destes roteadores, além de identificar o destino do pacote e encaminhá-lo na direção certa, eles checam ainda: a direção dos pacotes; de onde veio e para onde vai (rede interna e Internet); endereço de origem e destino; tipo de pacote; portas de conexão; e flags do pacote.

Estes pontos de conexão da Internet com a rede interna podem receber uma série de regras para avaliar a informação corrente. São as listas de acesso que definem o que deve e o que não deve passar por este ponto de conexão. Elas são mais ou menos assim:

# regra	s/ñ	Protocolo	origem	destino	opções

A opção "sim/não" equivale a "permitir a passagem do pacote/negar à passagem do pacote" e em "opções" definiremos os flags do pacote e portas de destino. Claro, esta é uma generalização das sintaxes mais comuns, o que nos permite ter uma idéia geral de como isto pode ser configurado.

Para impedir o acesso à rede interna, não permitindo conexões Telnet (pacotes TCPs da porta 23) com nossos hosts (pelo menos as conexões vindas da Internet). Colocamos filtros na interface de entrada dos pacotes externos na rede interna. Pela sintaxe do exemplo, ficaria assim:

# regra	s/ñ	protocolo	origem	Destino	opções
#1	ñ	TCP	qualquer	Interno	porta 23

Ou seja, negar todos os pacotes TCP para a porta 23 vindos da Internet em direção a qualquer máquina da rede interna. Porém, caso seja necessário este tipo de conexão, para realização de acessos remotos, por alguém da empresa, pode-se identificar de onde ele está tentando se conectar e permitir a entrada dos seus pacotes.

# regra	s/ñ ñ	protocolo	origem	Destino	opções
#1	s	TCP	qualquer	Interno	porta 23
#2		TCP	200.17.21.8	Interno	porta 23

Dessa forma, os pacotes vindo de 200.17.21.8 poderiam passar pelo roteador.

Baseado nesta ordem, podemos definir uma política para a segurança da rede. A primeira opção é liberar tudo e negar os serviços perigosos; a segunda é negar tudo e liberar os serviços necessários. Sem sombra de dúvidas, a segunda é mais segura, entretanto, a rede interna podem precisar acessar recursos livremente no Mundo Externo, e a manutenção desta lista seria tão trabalhosa, visto a proliferação de serviços que, em pouco tempo estaríamos completamente perdidos em um emaranhado de regras sem sentido.

Os roteadores verificam também os "flags do pacote". Um flag é uma sinalização entre os computadores intercomunicantes que identificam alguns estados em que o pacote se encontra. Os pedidos de conexão originais não possuem o flag ACK (de 'acknowledgment'), somente os de resposta.

# regra	s/ñ	protocolo	Origem	destino	opções
#1	s	IP	Interno	qualquer	
#2	s	TCP	qualquer	interno	flag ACK

Desta forma, todos os pacotes com o flag ACK ativado poderiam entrar na rede interna, mas os outros seriam bloqueados. É importante lembrar que estas regras se aplicam a cada interface do roteador, ou seja, a regra 1 seria aplicada na interface do roteador com a rede interna e, a número 2, na interface do roteador com a Internet. O sentido em que a informação passa pelo roteador deve ser levado (e muito) em consideração.

O autor do livro "Firewall - Repelling the wily hacker", Steve Bellovin, propôs a utilização de um recurso no FTP chamado "FTP Passivo" que resolveria este problema da filtragem de pacotes. Com este método, os clientes e servidores de FTP trocariam normalmente as informações mas, no momento de transferir o arquivo, quem faria o pedido de envio pela porta 20 seria o cliente. Com isto os pacotes do arquivo chegariam com o flag ACK acionado (já que agora se trata de uma conexão feita, e não mais de uma tentativa de estabelecê-la), e assim poderíamos impedir a conexão com todas as portas altas da sua rede Interna.

Os Filtros Inteligentes

Pensando nas dificuldades de configuração e falta de recursos dos roteadores para a implementação dos filtros de pacotes, muitos fabricantes criaram ferramentas para fazer este tipo de filtragem, desta vez baseada em um host (computador) específico para esta tarefa, localizado nos pontos de conexão da rede interna com a Internet.

Os chamados filtros inteligentes são aplicações executadas em, por exemplo, computadores ligados ao roteador e à rede interna. O tráfego de um lado para outro se dá (ou não) conforme as regras estabelecidas nas aplicações. Apesar desta solução requerer um equipamento extra, ela nos dá uma série de vantagens sobre os filtros baseados em roteador, principalmente no que diz respeito à monitoração de acesso.

Roteadores, quando possuem algum tipo de log, não guardam informações muito precisas sobre as tentativas de conexão na (ou da) rede interna, enquanto os filtros inteligentes possuem vários níveis de logs, nos quais é possível (e bastante recomendável) perceber os tipos de tentativa de acesso, e até definir certas ações caso um evento em especial relacionado à segurança aconteça.

Uma outra característica interessante dos filtros inteligentes é a tentativa de implementar um controle de pacotes UDP, guardando informações sobre eles e tentando "improvisar" o flag ACK. Montando-se uma tabela de pacotes UDP que passam, pode-se comparar os pacotes UDP que retornam e verificar se eles são uma resposta ou se são uma tentativa de novo contato.

2.8 Métodos de Segurança de Redes

2.8.1 Gerenciando a Segurança das Informações nas Empresas

A segurança da informação tem deixado de ser tratada como um assunto técnico do pessoal de informática, tornando-se uma prioridade do pessoal de negócios. Os executivos começam a valorizar os investimentos necessários, sendo que 80% planejam implementar

recursos adicionais de segurança nos próximos dois anos, segundo pesquisa recente da Sentry Market Research.

Outra recente pesquisa da Association for Federal Information Resource Management (AFFIRM), sobre as 20 principais tecnologias que ajudarão os executivos a realizarem seus objetivos, aponta a segurança dos sistemas como segunda prioridade (68%) atrás apenas da tecnologia Internet com 73%.

Neste contexto, a administração da segurança das informações nas empresas exige o conhecimento acumulado das principais ameaças e vulnerabilidades, padrões de referência (benchmarking) e processos para proteção e controle.

De um modo geral, segurança da informação é a garantia da integridade, confidencialidade e disponibilidade dos sistemas, infra-estrutura e informações da empresa. Para tal, é preciso levar em conta os processos envolvidos no tratamento, armazenamento e transmissão das informações, desde a sua criação até o descarte.

A real definição de valor da informação para a empresa, passa a ser considerado no inicio do processo de segurança, de forma a considerar o impacto no negócio nos casos de possíveis perdas e, com isto, dimensionar adequadamente os investimentos necessários para proteção e controle.

Este processo de medição do valor das informações na empresa é conhecido como análise de riscos, que pode ser feita de forma quantitativa (valores numéricos) ou qualitativa (baseado em graus de criticidade). Dos fatores considerados, encontram-se custos de reposição e aquisição em casos de perdas, custos de retrabalho, diminuição da produtividade, perdas de negócios ou contratos, indisponibilidade de serviços, danos à imagem, prejuízos em concorrências e licitações nos casos de vazamento de informações, enfim, todos os aspectos

do negócio que possam afetar a imagem e credibilidade da empresa ou causar prejuízos financeiros diretos com custos adicionais e redução das receitas.

Os executivos começam a sensibilizar-se cada vez mais para estes problemas na medida que os riscos passam a ser mais conhecidos através de matérias e notícias regulares na mídia. A Internet contribuiu bastante para o aumento deste nível de conscientização, com os hackers assumindo o papel de "inimigo número 1" das corporações. Apesar disto, sabemos que a maior parte dos crimes e prejuízos tem sido causada pelo próprio pessoal interno ou de alguma forma com o envolvimento deste.

As principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários que, inadvertidamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas ou mesmo contaminam seus arquivos e programas com vírus de computadores.

No nível mais técnico / operacional da informática das coorporações encontram-se ações eficientes e processos bem estruturados em segurança, apesar da falta de documentação. Ações isoladas de pessoas ou áreas em detrimento a políticas corporativas. Alguns exemplos destas ações são rotinas de backup nos servidores, procedimentos de atualização de versão de antivírus, procedimentos de cadastro (e remoção) de usuários, configuração de servidores, política de monitoração e planos de contingência e recuperação em casos de acidentes.

Estações totalmente abertas com dados em planilhas, textos e documentos gravados no disco local sem proteção de acesso ou controle de uso. Roteadores e outros equipamentos críticos estão conectados à Internet com senha padrão do fabricante. O nível de segurança dos servidores é normalmente o padrão de fábrica muitas vezes com auditoria desabilitada,

proteções inadequadas, usuários "convidados", sem aplicação de "patches" e com serviços e programas desnecessários.

As ameaças para a segurança, antes restritas a especialistas e profundos conhecedores, passam a estar presentes em ferramentas gratuitas disponíveis na Internet e distribuídas entre usuários. É o caso de programas para produção de vírus, roubo de senhas, grampos de rede, identificação automática de vulnerabilidades, ataques de paralisação de redes.

Os criminosos estão se aperfeiçoando com técnicas e ferramentas para violar os sistemas das empresas, praticar vandalismo , cometer fraudes, extorsões e roubo de informações.

Para reverter este quadro e garantir que a segurança esteja prevista nos projetos desde os primeiros momentos de especificação, torna-se necessária uma Política de Segurança Corporativa. Esta política deve conter diretrizes, normas, procedimentos, produtos, estruturas gerais de segurança, além de um programa de conscientização e mensagem executiva da alta administração demonstrando apoio à política, sem o qual não se consegue a adesão necessária.

As responsabilidades e penalidades também devem estar previstas segundo a filosofia, normas administrativas e código de conduta empresarial de cada empresa. O momento é crítico pois ao mesmo tempo em que aumenta o número de negócios on-line, os riscos crescem a cada dia e os usuários sentem-se desprotegidos, a espera de orientação quanto aos critérios e medidas a utilizar. Não basta proteger as informações e sistemas atuais, é preciso conhecer e entender as novas ameaças e vulnerabilidades que vão surgir no futuro. As empresas assistirão o aumento de fraudes em transações eletrônicas, quebra de privacidade em e-mails, extorsões, roubo de segredos industriais e uso indevido de seus sistemas e infra-estrutura de tecnologia da informação.

É preciso ter uma visão macro do que vem a ser segurança da informação. Fazendo uma analogia, a segurança seria uma corrente composta por diversos elos, que seriam os pontos vulneráveis merecedores de atenção. Neste conceito de corrente, existe a preocupação de manter o mesmo nível de segurança para cada elo, pois de nada adiantará elos extremamente fortes, se um único estiver fraco e vulnerável. Estes detalhes, que muitas vezes passam desapercebidos ou recebem pouca atenção, e que podem comprometer todo o investimento em segurança realizado, representando grandes vulnerabilidades.

O usuário também é um elo da corrente, mesmo que o servidor esteja bem configurado, o e-mail seguro, o lixo informático fragmentado, e os backup realizados com exatidão, é necessário ainda uma política de segurança que sirva como bússola, definindo diretrizes, responsabilidades, normas e procedimentos para a melhor utilização do ambiente informatizado.

2.8.2 Política de Segurança

Política de Segurança é o conjunto de decisões que, coletivamente, determinam a postura de uma organização em relação à segurança. Mais precisamente, uma política de segurança determina os limites aceitáveis de comportamento e práticas, e as medidas a serem tomadas no caso da sua violação.

Os principais objetivos de uma política de segurança são os de definir as expectativas da organização quanto ao uso dos seus computadores e rede, e de estabelecer procedimentos visando prevenir e responder a incidentes relativos a segurança. Entre eles: definir uma política de segurança; e definir os mecanismos para implementar esta política.

A criação de uma política precisa ser um esforço conjunto entre o pessoal técnico e o pessoal responsável pelas decisões na organização, realizando uma análise de riscos, implementado medidas de proteção, observando o custo-benefício e revisando o processo continuamente e melhore toda a vez que for encontrada uma fraqueza

Atualmente há dois paradigmas que regem o ponto de partida para a definição de uma política de segurança:

O que não está expressamente permitido, é proibido

O que não está expressamente proibido, é permitido.

Observe que cada cooporação possui problemas diferentes no que tange à segurança. À parte chave na criação de uma política de segurança é fazer uma avaliação de riscos, para decidir o que realmente precisa ser protegido e a quantidade de recursos que deve ser usado para protegê-los.

Análise de Riscos

A análise de Riscos envolve determinar o que você precisa proteger, de quem você precisa proteger, e como deve ser protegido, além de qual o valor do que precisa ser protegido.

Certamente que se precisa proteger o Hardware (Cpus, teclados, roteadores, linhas de comunicação), Softwares (Software: Fontes, utilitários), Dados (Backups, logs, bases de dados;), Pessoas (Usuários, pessoas que precisam usar o sistema), Documentação (de programas, administrativo) e Material (papel, formulários, mídia magnética) dos diversos tipos de ameaças, ou seja: Acesso não autorizado; Uso de conta de outro usuário para ganhar acesso ao sistema. O acesso não autorizado abre uma porta para outras ameaças à segurança.

Para alguns sites, o simples fato de alguém ganhar acesso não autorizado já é um dano irreparável, com isso é possível: Descoberta de Informações; Você deve poder determinar o valor da informação contida nos seus computadores; Assim como a descoberta de um arquivo de passwords pode permitir futuros acessos não autorizados, um paper técnico pode conter anos de pesquisa; Indisponibilidade de Serviço.

Os computadores e redes provêem inúmeros serviços a seus usuários. A indisponibilidade destes com certeza resultará em perda de produtividade. Cada site deve determinar quais serviços são essenciais, e o que será afetado se este serviço for desabilitado.

Se o administrador sente que seu site está vulnerável, ele pode escolher uma alternativa do tipo "Proteger e continuar". Caso o administrador sinta-se capaz de identificar a origem do ataque, ele pode optar por "Perseguir e processar" o culpado, através da permissão controlada da intrusão, até identificar os culpados.

Identificação das Aplicações Críticas

Podemos classificar as aplicações em 3 níveis de prioridade de processamento:

aplicações críticas (prioridade máxima de processamento);

aplicações semi-críticas (prioridade média de processamento);

aplicações não-críticas (prioridade mínima de processamento);

Aplicações críticas

Existem duas correntes de pensamento sobre o que é uma aplicação crítica: a) Uma aplicação é considerada crítica em função do tempo de paralisação que ela pode suportar e da data(mês, dia) e hora que a paralisação ocorre. b) Uma aplicação crítica é aquela que não

suporta paralisação, independemente da hora da paralisação. Uma aplicação crítica é crítica a qualquer momento.

As aplicações críticas são aquelas:

essenciais para a sobrevivência da empresa;

cujo processamento não pode paralisar;

cujo custo de paralisação é muito alto;

cuja paralisação requer o uso de recursos alternativos para a continuidade do processamento.

A determinação das aplicações críticas a serem cobertas pela Política de Segurança deve resultar de uma avaliação criteriosa e de um consenso entre a gerência de informática, gerências usuárias e diretoria da empresa.

A Necessidade de Conscientização

A empresa deve, através de relatório(s) à alta administração e à gerência do CPD:

mostrar os inúmeros e sérios riscos a que está sujeito o ambiente de computação da empresa;

mostrar os inúmeros e sérios riscos a que está sujeita a empresa, caso ocorra paralisação prolongada dos sues recursos de computação;

lembrar que segurança é uma preocupação administrativa e não técnica;

lembrar que cabe a todos a responsabilidade de proteger os empregados, bens, serviços e informações da empresa;

recomendar a implementação de efetivas medidas de segurança, visando a prevenção contra riscos no ambiente computacional;

lembrar que é necessário garantir o processamento das aplicações críticas, para assegurar a continuidade das atividades e negócios essenciais da empresa;

recomendar a elaboração e implementação de um plano de Contingência para Informática.

A gerência de informática deve, através da sua equipe de administração (ou coordenação) de segurança, conduzir um efetivo trabalho de conscientização, junto às gerências dos departamentos usuários e junto à alta administração, sobre a importância de uma Política de Segurança. Para tanto, deve se utilizar de reuniões, palestras, visitas, correspondências, relato de fatos já publicados, etc.

3 Estudo de Caso (Rede UNOESC – São Miguel)

3.2 Histórico da UNOESC São Miguel

Os miguelestinos tinham um sonho, trazer o Ensino Superior para a região. Alguns referenciais que transformaram o sonho em realidade:

Em abril de 1974, foi aprovada a Lei nº 878, criando a FUNESC;

Em 1978, o 1º Conselho Implantador da FUNESC firmou convênio com a FUNDESTE para elaborar projeto de viabilidade técnica-financeira, visando demonstrar condições de implantação de Faculdade;

Em 1981, reiniciam-se as negociações FUNDESTE elabora novo projeto - Cedência de vagas por tempo determinado;

Em 1982, Legislação Federal proíbe a implantação de cursos fora da sede;

Em 1983, Legislação Federal possibilita a transferência de vagas;

17 de dezembro de 1985, - parecer nº 411/85 aprovando a implantação do Ensino Superior, com o curso de Administração de Empresas em São Miguel do Oeste. É assinado pelo então presidente do CEE, Sr. Antônio Osvaldo Conci;

1986, Sr. Luiz Basso, Prefeito Municipal viabiliza o 1º ingresso;

24 a 27 de fevereiro de 1986 - 1° Concurso Vestibular;1988, 1° ingresso do curso de Pedagogia;

1995, 1° ingresso do curso de Ciências Contábeis;

1996, 1° ingresso dos cursos de Geografia, Letras - Habilitação Espanhol, Matemática, Administração - Ênfase Rural (Maravilha) e Pedagogia (em Itapiranga);

Quando as Fundações integraram-se para constituir a UNOESC, os Departamentos foram instituídos como unidades básicas de organização.

Nesta época, no Campus de São Miguel do Oeste, os dois cursos existentes, Administração de Empresas e Pedagogia, deram origem aos Departamentos de Ciências Administrativas e Ciências da Educação, respectivamente. Com a expansão dos cursos de graduação, sentiu-se a necessidade de reestruturar os departamentos, o que aconteceu no final do mês de novembro de 97.

1997, 1° ingresso dos cursos de Direito e Letras - Habilitação em Alemão;

1998, 1° ingresso dos cursos de Tecnólogo em Informática e Educação Artística - Habilitação Artes Plásticas;

1999, 1° ingresso dos cursos de Educação Física, Letras - Habilitação Inglês e Pedagogia (Maravilha).

Até 1999 o Campus possuía os seguintes departamentos:

Departamento de Ciências Administrativas;

Departamento de Ciências da Educação;

Departamento de Ciências Contábeis;

Departamento de Ciências da Comunicação;

Departamento de Ciências Jurídicas;

Departamento de Ciências Humanas e Sociais;

Departamento de Ciências Exatas.

A reforma estatutária aprovada pela Resolução nº 52/CONSUN/99, altera a estrutura organizacional da UNOESC.

Os departamentos, foram agrupados por área de conhecimento, respeitando as peculiaridades de cada campus, constituindo os Centros.

Como foram constituídos os Centros na UNOESC – São Miguel.

Centro de Ciências Sociais Aplicadas

Centro de Ciências da Educação

Centro de Comunicação e Artes

Centro de Ciências Sociais e Jurídicas

3.3 Histórico da Rede UNOESC – São Miguel

A Rede UNOESC – São Miguel iniciou de forma bastante modesta, porém, seu crescimento gradativo demonstra exatamente sua demanda por novos serviços, recursos físicos, humanos, etc.

Desde o seu início, a Rede UNOESC – São Miguel, tem como modelo um sistema de computação distribuído de rede.

Para a melhor visualização da evolução histórica dos recursos de informática na Universidade do Oeste de Santa Catarina – Campus de São Miguel do Oeste, bem como as transições de tecnologias, apresentamos os dados em forma cronológica.

1992 – Aquisição do primeiro microcomputador da UNOESC, (IBM PC compatível - 80286) utilizado para controles administrativos.

1993 – Aquisição de 05 microcomputadores (IBM PC compatíveis – 80386 e 80486). Estes equipamentos foram colocados em rede, utilizando-se a topologia física de barramento, e a plataforma de software foi Windows 3.11. Expandiu-se com isso a utilização a nível administrativo e iniciou-se o processo de informatização da Biblioteca e Departamentos Acadêmicos.

1995 – Aquisição de 08 microcomputadores (IBM PC compatíveis – 486, Pentium 75, Pentium 100) e 01 servidor (IBM PC compatíveis – 486) com o Sistema Operacional de Rede - Novell Netware 3.12. Implementaram-se então diversos serviços de rede, entre eles Servidores de Arquivos, Servidor de Aplicação e Servidor de Impressão. Alguns destes equipamentos integraram as redes já existentes e outros ficaram trabalhando de forma isolada (standalone).

1997 – Aquisição de 30 microcomputadores (IBM PC compatíveis –Pentium 166) e 02 servidores (IBM PC compatíveis – Pentium 200). Neste período foram realizadas a

substituição do hardware do Servidor Netware (486 para Pentium 200) e instalado um novo servidor, em outra plataforma de software (Pentium 200 com Windows NT 4.0). 23 máquinas passaram a compor o primeiro laboratório de informática do Campus.

Ainda Neste ano, foram adquiridos equipamentos para interconexão de redes, sendo 01 switch modular, 08 hubs, totalizando uma capacidade de conexão de 116 pontos de rede.
Os blocos mais distantes foram conectados através de fibra ótica ao switch central.
Toda a rede estava focada em uma topologia física tipo estrela, utilizando-se de cabeamento estruturado.

1998 – Aquisição de 20 microcomputadores (IBM PC compatíveis –Pentium 166 MMX e Pentium 200 MMX). Ligação da Rede UNOESC – São Miguel ao projeto RCT-SC, passando integrar a rede mundial e a fornecer serviços de WWW, FTP e Mail. Aquisição e implantação de servidor de banco de dados (Pentium II 266(DUAL),

1999 – Liberação do acesso doméstico a internet. Implantação de sistemas coorporativos. Troca do sistema da biblioteca para ambiente de banco de dados. Aquisição de 50 computadores (Pentium III 450), sendo que 30 passaram a constituir o Laboratório de Informática do Curso de Tecnólogo em Informática.

2000 – Troca de sistemas coorporativos, nova plataforma e Banco de Dados, com conceito de ERP. Aquisição de 35 computadores (Pentium III 500), sendo que 20 passaram a constituir o Laboratório de Informática do Curso de Ciências Contábeis. Implantação de diversas soluções de menor porte utilizando-se o sistema operacional de rede Linux. Aquisição de 03 switchs para composição do Backbone do Campus, passando este para 100 Mbits.

3.4 Subredes da Rede UNOESC – São Miguel

Atualmente a Rede UNOESC – São Miguel é composta por 04 sub-redes, interligados a um backbone central em 100 Mbits (fig. 1).

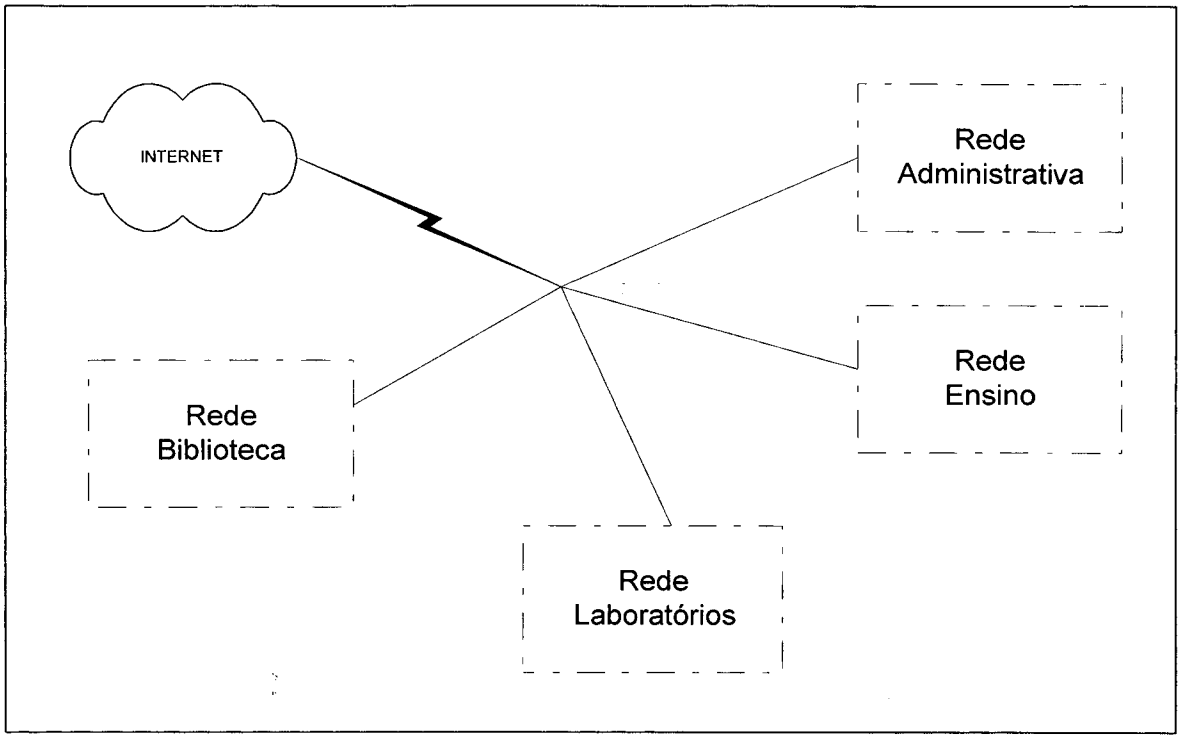

Fig 3.1 – Esquema das Sub-redes da Rede UNOESC – São Miguel

3.5 Infra-Estrutura da Rede UNOESC – São Miguel

A figura 2 apresenta o backbone da Rede UNOESC – São Miguel que é composto por um switch central onde estão conectados diversos outros switches, e a estes, por sua vez, estão conectados os demais hubs e switches. O protocolo utilizado é o TCP/IP.

Os hosts da rede utilizam-se de um endereço IP de classe C válido na Internet para uso tanto na rede interna quanto para acesso à Internet. Este endereço de classe C é fornecido pela RCT-SC para uso da UNOESC no acesso à Internet.

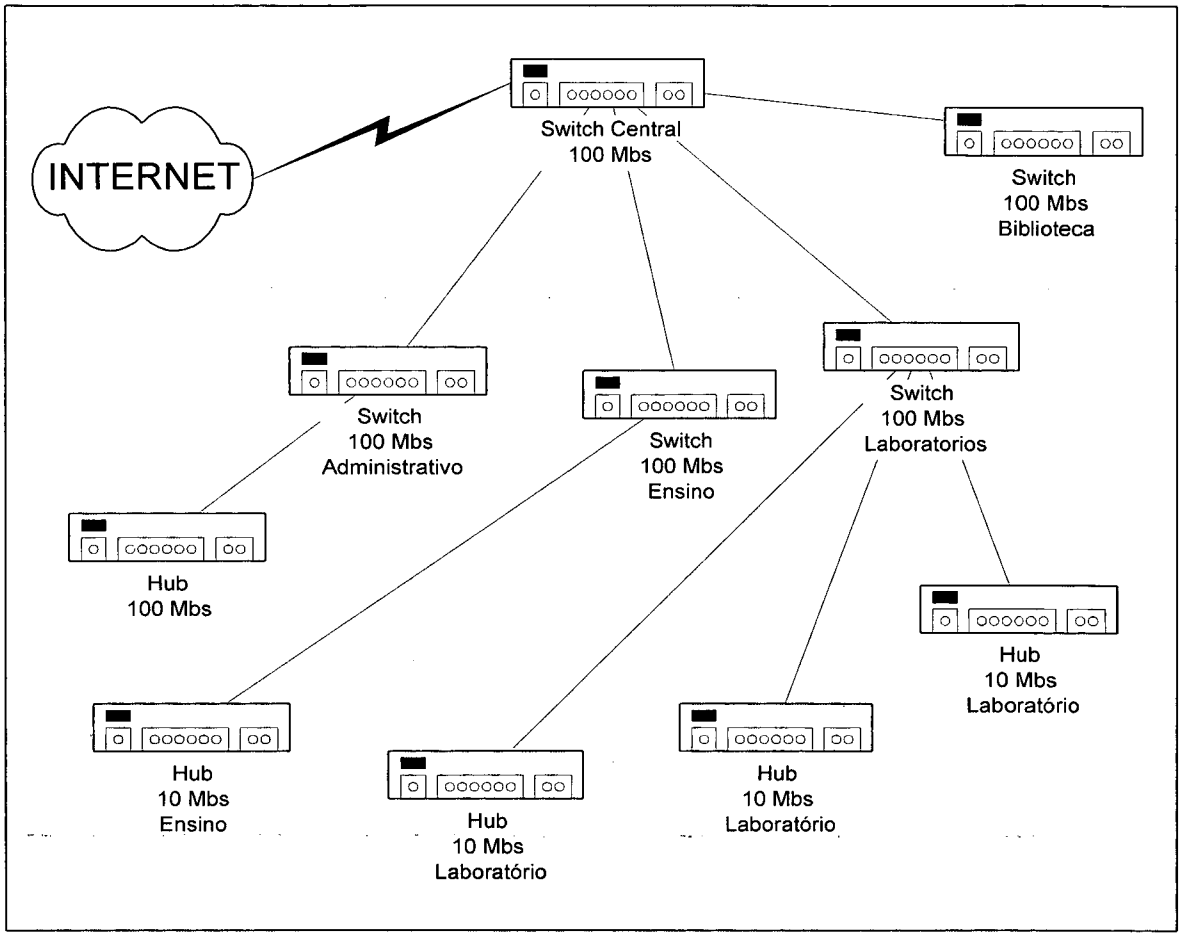

Fig 3.2 – Backbone atual da Rede UNOESC – São Miguel

Todos os computadores da rede possuem acesso à Internet e aos recursos disponibilizados na rede, obtendo acesso através aos servidores de aplicações, banco dados, arquivos e Internet, permitindo o acesso a diversas informações.

3.6 Número de Equipamentos interconectados

A Rede UNOESC – São Miguel possui aproximadamente 147 computadores interconectados, distribuídos da seguinte forma:

Estrutura Administrativa

- Servidores de Banco de Dados
- Servidores de Aplicações
- 37 estações / microcomputadores

Estrutura Internet

- Servidor WWW, FTP, Mail
- Roteador Cisco 2511
- 16 modems para acesso discado

Estrutura Acadêmica

- Servidor de Arquivos
- 30 estações / microcomputadores

Estrutura Laboratorial

- Servidores de Arquivos dos Laboratórios
- Servidores de Impressão dos Laboratórios
- 73 estações / microcomputadores

3.1.1. Estrutura Administrativa

A estrutura administrativa é composta pelos setores que realizam as tarefas rotineiras de administração da instituição, sendo eles: Contabilidade, Tesouraria, Serviços Gerais, Serviço de Apoio ao Estudante, etc. Fazem acesso a sistemas no Servidor de Aplicação, acesso a documentos no servidor de arquivos e interagem com o servidor de banco de dados. Além de utilizarem-se da Internet para os mais variados fins, e de forma transparente.

3.1.2. Estrutura Acadêmica.

Esta é composta pelos setores que respondem pelas atividades acadêmicas da instituição. Podemos citar entre eles a SERCA – Secretaria de Registro e Controle Acadêmico, a Biblioteca Universitária, os Centros de Ensino, Coordenações de Cursos e setores de Pós-Graduação, Pesquisa e Extensão, utilizando-se igualmente de forma transparente os servidores de Banco de Dados, Aplicação e Arquivos.

3.1.3. Estrutura Laboratorial.

Os laboratórios de Informática da Universidade do Oeste de Santa Catarina, Campus de São Miguel do Oeste, proporcionam o acesso aos recursos tecnológicos disponíveis a comunidade acadêmica, para aulas, pesquisas e trabalhos extra classe.

3.7 Níveis de utilização de recursos e Interoperabilidade

3.7.1 Níveis de Utilização

Os níveis de utilização dos recursos fornecidos pela UNOESC – São Miguel, em sua rede são relativamente pequenos. O aumento da demanda por serviços on-line e a disponibilização, por parte da instituição, de diversos produtos que utilizam o meio Internet está gerando uma demanda crescente pela utilização desta infraestrutura fornecida.

A possibilidade dos alunos realizarem consultas de informações, alterações em cadastros, matrículas e outros, através da internet já são uma realidade. Com a popularização de tecnologias de desenvolvimento de soluções voltadas para a internet, como sites de e-commerce (B2B, B2C, etc), visualiza-se um rápido crescimento na utilização dos recursos.

3.7.2 Interoperabilidade

A estrutura apresentada, demonstra a grande interação existente entre os diversos serviços da rede, sobretudo considerando a conexão permanente destes sistemas com a Internet. Isto acarreta uma troca constante de informações entre os serviços, hosts e dispositivos da rede.

3.7.3 Problemas apresentados na estrutura atual

A estrutura da rede utilizada atualmente revela problemas de segurança. A utilização de endereçamento IP válido na interne (classe C) permite que quaisquer hosts da rede interna sejam visualizados tanto da própria rede interna quanto da internet, tornando-se desta forma, um alvo para tentativas de invasão.

Deste modo, através de técnicas de escuta dos pacotes que trafegam pela rede, pode-se facilmente identificar os IPs dos hosts da Rede UNOESC e efetuar diversas tentativas sejam elas de invasão, negação de serviços ou captura de informações.

Considerando que a utilização dos equipamentos conectados a rede interna é feito tanto para tarefas administrativas quanto para fornecimento de estrutura para o ensino, temos uma realidade onde não apenas o ambiente externo mostra-se hostil, à parte da rede interna que compreende os laboratórios de informática são oferecidos como instrumentos para tentativas de invasão da Rede UNOESC, transformando-se então, hostil na mesma proporção da Internet.

4 Proposta de um modelo para proteção das informações

Para a proposição de um modelo para melhorar a segurança (proteção) e disponibilidade das informações que trafegam na Rede UNOESC, consideramos dois aspectos principais, sendo eles a configuração física de rede UNOESC e as Políticas Administrativas necessárias para que as melhorias possam surtir os efeitos a que se destinam.

4.2 Configuração física da rede

O modelo de configuração física da rede proposto pode ser observado na figura 2 e consiste na utilização de técnicas baseadas em Segmentação de Redes, Firewall e Proxy.

4.2.1 Segmentação da Rede

Na segmentação das redes, utilizou-se a divisão da rede interna em três grandes grupos: a Rede Administrativa, a Rede Acadêmica ou Laboratorial e a Rede Internet. Estas redes passam a estar fisicamente separadas, interconectadas através de um nov host que assumira a função de gateway.

A Rede Administrativa contempla os setores que realizam as atividades relacionadas à administração da instituição e que prestam serviços aos alunos, sendo eles: Contabilidade, Tesouraria, Secretaria Acadêmica, Centros de Ensino, Coordenação de Cursos, Biblioteca Universitária, Programa de Avaliação Institucional e Serviço de Apoio ao Estudante.

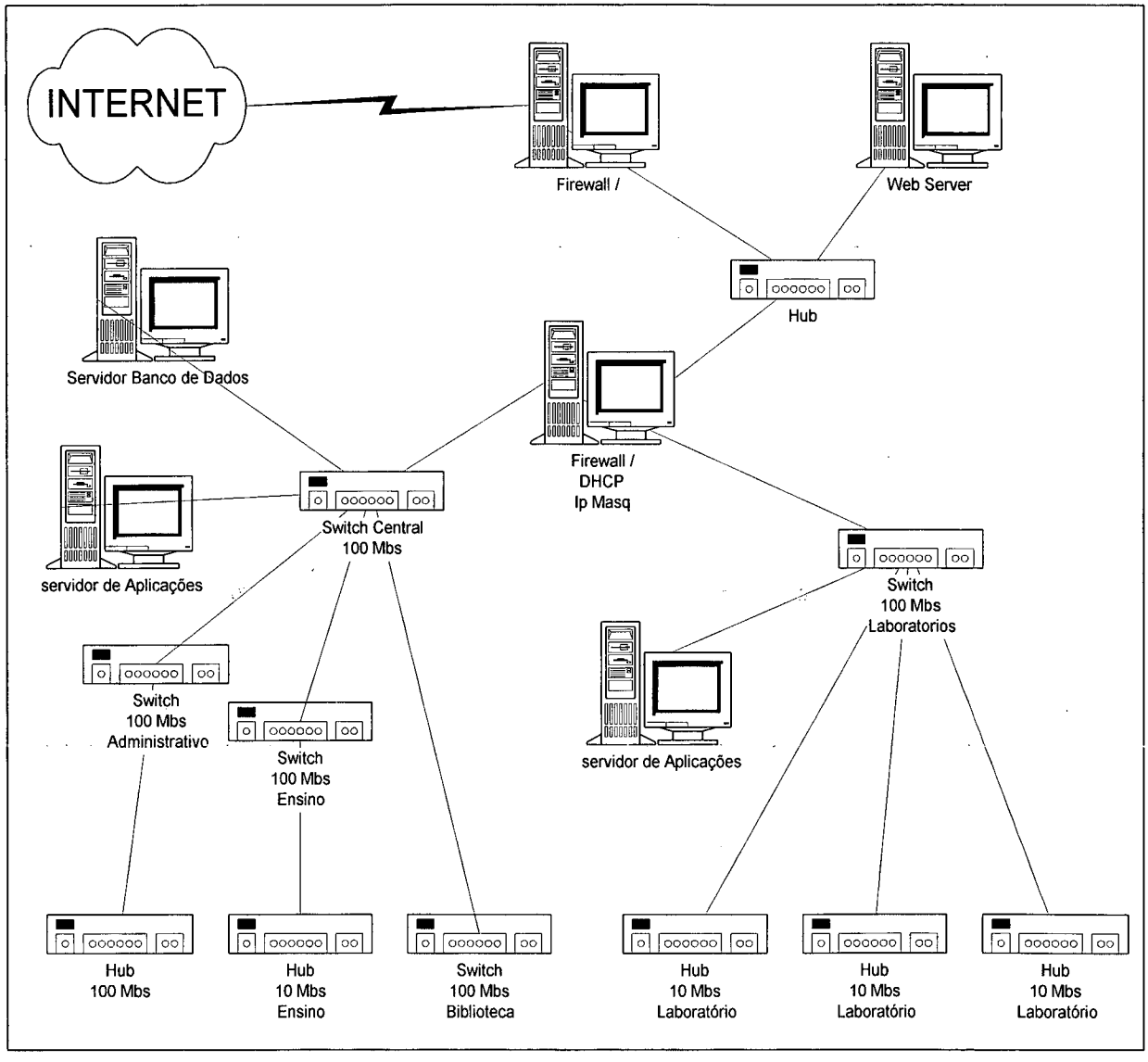

Figura 4.1: Modelo de rede proposto

A Rede Acadêmica ou Laboratorial engloba os Laboratórios de Informática da UNOESC que são de uso acadêmico.

A Rede Internet mantêm consigo os equipamentos responsáveis pelos serviços de internet, sejam eles DNS, mail, FTP, conexão discada e roteadores.

Esta divisão possui fundamental importância no modelo da solução, pois é baseado nela que se tem ha implementação do sistema de segurança.

Através da segmentação da rede, consegue-se utilizar classes de ip inválidos (Classe B) para as Redes Administrativa e Acadêmica, viabilizando assim, a primeira instância de proteção da Rede UNOESC, pois estas duas redes não mais serão vistas da Internet.

Desta forma, todo pacote enviado por quaisquer hosts das redes Administrativa ou Acadêmica leva no cabeçalho o seu endereço IP inválido (192.168.x.x por exemplo). Ao passar pela máquina gateway recebe a tradução do cabeçalho e passa a ter endereço IP válido para continuar trafegando para a rede Internet e rede externa (Internet). Quando a resposta à solicitação retornar, o gateway traduz inversamente o cabeçalho, remetendo ao host de origem.

4.2.2 Firewall

A solução de Firewall contempla duas fases distintas: Firewall da Rede Externa e Firewall da Rede Interna.

Na Rede Interna, em conjunto com o a segmentação de redes, na máquina gateway, é uma solução do tipo firewall atuando na camada Internet do protocolo TCP/IP, fará a filtragem dos pacotes. As regras implementadas farão com que seja possível um controle

efetivo de quais pacotes poderão passar de uma rede para outra e, da mesma forma, quais não deverão ter acesso.

Esta implementação pode atuar tanto no bloqueio / liberação de determinados IPs quanto no bloqueio / liberação de determinados serviços requisitados (telnet, finger, etc).

Na rede Externa, um outro equipamento, atuando como firewall, da mesma forma, na camada Internet do protocolo TCP/IP, realizará a filtragem de pacotes, bloqueando / liberando as requisições feitas da Internet como um todo para dentro da Rede UNOESC.

4.2.3 Proxy

O serviço de proxy é implementado na máquina gateway realizando o cache de conteúdo recebido da Internet (WEB). Também, nesta solução, é possível o filtro de url especificando conteúdos que podem ou não ser acessados.

Quaisquer requisições de serviços WEB feitos na rede interna são repassados para o proxy, que fará uma rápida conferência no site de destino para checar a atualização do mesmo. Estando o conteúdo local atualizado, será retornado imediatamente ao solicitante, sem a necessidade de download desta requisição da Internet. Em caso de estar desatualizado, o proxy fará o download, atualizando sua base e repassando as requisições ao solicitante.

A outra função do proxy. consiste no filtro do conteúdo requisitado. Pode-se verificar individualmente cada requisição e realizar a filtragem daquilo que não se deseja disponibilizar aos usuários. Para isto são definidas as regras de permissão e negação de conteúdos..

4.3 Políticas Administrativas da rede

As Políticas administrativas relativas à rede, seu uso, os direitos e obrigações dos usuários, deverão ser contempladas por dois mecanismos, a Política de Segurança e o Plano de Contingências.

4.3.1 Política de Segurança

A UNOESC – São Miguel possui um Manual de Segurança de Informações que contem diversos aspectos referentes à segurança, praticamente contemplando toda a gama de informações para os usuários. De fato, este material não é utilizado como ferramenta preventiva de segurança.

Com a rotatividade de pessoal, o número de pessoas que tem conhecimento deste documento reduz com o passar do tempo, acarretando no desconhecimento das normas e procedimentos relativos à segurança de informação.

É necessária a reativação desta função de conscientização dos usuários, principalmente para dar efetividade as ferramentas apresentadas nesta solução.

4.3.2 Plano de Contingências.

O plano de contingências tem como objetivo a definição dos procedimentos

emergenciais que deverão ser realizados no momento em que alguma falha ou contingência ocorrer em nível de estrutura de informática ou da informação.

A efetiva construção destes procedimentos deverá levar em conta as características do ambiente computacional aqui descrito, bem como as responsabilidades e atitudes de cada pessoa envolvida nos processos.

5 Conclusão

Podemos concluir que o modelo apresentado é viável e de real importância para a Rede UNOESC, uma vez que permite um elevado grau de disponibilidade das informações e contempla níveis de segurança ideais.

Destacamos que, com esta solução, passa a ser possível a disponibilização de uma enorme gama de serviços on-line por parte da UNOESC, haja vista que passamos a ter um ambiente seguro de forma suficiente, e, principalmente, esta segurança não comprometendo a disponibilidade de informações.

A implementação destes modelos está em andamento através de incentivo a alunos de graduação da Universidade, que na forma de Trabalhos de Conclusão de Curso, implementam na prática estas soluções.

6 Sugestões para Trabalhos Futuros

Como sugestões para trabalhos futuros, deixamos alguns itens que, sejam por motivo de tempo ou da limitação do escopo do trabalho, não foram contemplados neste.

- Efetivação do Plano de Contingências
- Implementação de Criptografia de dados
- Implementação de Certificados Digitais para autenticação

7 Referências

ALBUQUERQUE, Roger. **Spoofing do IP**. Disponível em <http://www.elogica.com.br/users/r0g3r/spoofing.htm>. Acesso em: 03 ago. 2000.

BISOTTO, Gisa Striquer; GASPARINI, Isabela; CHIBA, Lílian Mitsue; CEREZINI, Maria Angélica. **TCP/IP e FTP**. Londrina, Universidade Estadual de Londrina, Centro de Ciências Exatas, Departamento de Computação. Disponível em <http://proenca.uel.br/curso-redes-graduacao/1998/trab-08/equipe-01/>. Acesso em: 28 jul. 2000.

BRITO, Fábio Luis de. **O Modelo de Referência para Interconectividade de Sistemas Abertos**. São Paulo, Faculdade Leonardo da Vinci. Disponível em <http://orbita.starmedia.com/~falbrito>. Acesso em 07 mai. 2000.

CAMPBELL, Patrick T. **Instalando redes em pequenas e médias empresas**. Tradução Carlos Antonio de Mello. São Paulo: MAKRON Books do Brasil, 1997.

CAMPOS, Augusto C. Questão de bom senso. **Revista do Linux**, Curitiba, n. 7, p. 38-42, 2000.

CARVALHO, T. C. M. B. et alli. *Arquiteturas de Redes de Computadores: OSI e TCP/IP*, Ed. Makron Books, São Paulo, 1994.

CHIOZZOTO, Mauro; SILVA, Luís Antonio Pinto da. **TCP/IP - Tecnologia e Implementação**. São Paulo: Érica, 1999.

COMER, Douglas E. **Interligação em Rede com TCP/IP**. Rio de Janeiro: Campus, 1998.

COX, Guilherme. **Métodos de implementação de Firewall num ambiente Linux usando ipchains**. Disponível em <http://200.231.246.92/ seguranca/10 até http:// 200.231.246.92/seguranca/13>. Acesso em: 05 mai. 2000.

CYCLADES BRASIL. **Guia Internet de Conectividade.** 5. ed. São Paulo: Cyclades Brasil, 1999.

CRUZ, Anamaria da Costa; PEROTA, Maria Luiza Loures Rocha; MENDES, Maria Tereza Reis. **Elaboração de Referências**: NBR 6023: 2000. Rio de Janeiro: Interciência, 2000.

CURTY, Marlene Gonçalves; CRUZ, Anamaria da Costa. **Apresentação de trabalhos científicos**: guia para alunos de cursos de especialização. Maringá, PR: Dental Press, 2000.

FEGHHI, Jalal; WILLIAMS, Peter; FEGHHI, Jalil. **Digital Certificates**: Applied Internet Security. New York: Addison-Wesley, 1998. 453p.

GARGAGLIONE, Bruno Diégoli; PAULA, Pedro Castanheira de. **VÍRUS**: uma ameaça letal. Rio de Janeiro: Brasport, 1999.

GASPARINI, Anteu Fabiano L; BARRELA, Francisco Eugênio. **A Infraestrutura de LANs**. 2. ed. São Paulo: Érica, 1997.

_____. **TCP/IP**: solução para conectividade. 3. ed. São Paulo: Érica, 1993.

_____; BORTOLLI, Luis Fernando de; DAL´BÓ, Paulo Henrique. **Projetos para Redes Metropolitanas e de Longa Distância MAN, Campus e WAN Backbone Designer**. São Paulo: Érica, 1999.

GIL, Antônio de Loureiro, *Segurança em Informática*. Ed. Atlas, São Paulo, 1994.

GIOZZA, W. F. et alli. *Redes Locais de Computadores - Tecnologia e Aplicações*, McGraw-Hill, São Paulo, 1986.

GONÇALVES, Marcus. **Segurança na INTERNET**: protegendo seu web site com Firewalls. Rio de Janeiro: Axcel Books do Brasil, 1997.

GRANT, Gail L. **Understanding Digital Signatures**: Establishing Trust over the Internet and Other Networks. New York: Computing McGraw-Hill, 1997. 304p.

HELD, Gilbert. **Comunicação de Dados**. Tradução da 6ª edição original de Vandenberg Dantas de Souza. Rio de Janeiro: Campus, 1999.

JÚNIOR, José Helvécio Teixeira; SUAVÉ, Jacques Philippe; MOURA, José Antão Beltrão; TEIXEIRA, Suzana de Queiroz Ramos. **Redes de Computadores - Serviços, Administração e Segurança**. São Paulo: Makron Books do Brasil, 1999.

LIMA, Marcelo Barbosa. Anatomia de um ataque. **Revista do Linux**, Curitiba, n. 6, p. 50-54, 2000.

_____. Firewall: Uma Introdução à Segurança. **Revista do Linux**, Curitiba, n. 2, p.14-18, 2000.

_____. Firewalls a partir do IP Masquerade. **Revista do Linux**, n. 4, p. 14-17, 2000.

_____. Internet fácil, fácil. **Revista do Linux**, Curitiba, n. 3, p. 44-47, 2000.

MURILO, Nelson. As novas técnicas dos hackers. **Revista do Linux**, n. 4, p. 40-42, 2000.

OAKS, Scotr. **Segurança de dados em Java**. Rio de Janeiro: Ed. Ciência Moderna, 1999. 433p.

PEARSON, Oskar. **Squid. A User´s Guide**. Disponível em <http://squid-docs.sourceforge.net/latest/html/book1.htm>. Acesso em: 23 jun. 2000.

PFLEEGER, Charles P. **Security in Computing**. New Jersey: Prentice Hall, 1996. 574p.

RANCH, David. AMBROSE, Au. **Linux IP Masquerade HOWTO**. Disponível em <http://linux.lcmi.ufsc.br/doc/HOWTO/em-html/IP-Masquerade-HOWTO.html>. Acesso em: 05 ago. 2000.

RUSSEL, Paul. **Linux IP Masquerade HOWTO**. Disponível em <http://zeus.rmc.eti.br/library/linux/how-tos/IPCHAINS-HOWTO>. Acesso em: 05 ago. 2000.

RUDNIANSKI, M. *Architecture de Réseaux: le modèle ISO - Rôle et Fonctionnalités*, Editests, Paris, 1986.

SCHNEIER, Bruce. **E-Mail Security**: How to Keep Your Electronic Messages Private. New York: John Wiley & Sons, 1995. 384p.

SILVA, Cândido Fonseca da. **Sniffing**. Disponível em <http://inf.unisinos.br/pos-redes/seguranca/sniffer/funciona.htm>. Acesso em: 30 set. 2000.

SOARES, Luiz Fernando Gomes. LEMOS, Guido. COLCHER, Sérgio. **Redes de Computadores**: das LANs, MANs e WANs às Redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

SOUZA, Lindeberg Barros de. **Redes de Computadores**: dados, voz e imagens. 2. ed. São Paulo: Érica, 1999.

SPOHN, Marco Aurélio. **Internet Firewall**. Arquitetura TCP/IP. Porto Alegre, Universidade Federal do Rio Grande do Sul. Disponível em: <http://penta.ufrgs.br/redes296/firewall/fire.html>. Acesso em: 19 jul. 2000.

SPYMAN. **Manual Completo do Hacker**. 3. ed. Rio de Janeiro: Book Express, 2000.

STALLINGS, William. **Cryptography and Network Security**: Principles and Practice. Prentice Hall, 1999. 569p.

STINSON, Douglas R. **Cryptography**: Theory and Practice. New York: CRC Press, 1995. 448p.

TANENBAUM, A. S. *Computer Networks*, 3ª Ed, Ed. Prentice Hall, New York, 1996.

TEIXEIRA, José H. et alli. *Redes de Computadores: Serviços, Administração e Segurança.* Makron Books, São Paulo, 1999.

THOMAS, Robert M. **Introdução às Redes Locais**. Tradução José Carlos Barbosa dos Santos. Revisão Técnica Mario Magyar Franco. São Paulo: Makron Books, 1997.