SEGURANÇA EM REDES DE COMPUTADORES COM USO DE FIREWALLS

Paulo Henrique MARIOTTO NAHES [*]
Marco Antonio ALVES PEREIRA [**]

"O Universo por nós conhecido é apenas uma versão beta."
Autor Desconhecido

RESUMO

Este artigo aborda resumidamente a história das redes, como elas surgiram e como se deu a sua evolução. Trata também de um conjunto de informações e técnicas, relacionadas à segurança das redes, em que recursos e informação são compartilhados, com o intuito de proporcionar e esclarecer alguns problemas relativos à segurança, evitando muitas vulnerabilidades às quais as mesmas estão sujeitas.

PALAVRAS-CHAVE: Redes. Segurança. Configuração. Evolução. Firewall.

BREVE HISTÓRIA DAS REDES DE COMPUTADORES

Como tudo na informática, as redes passaram por muitas transformações durante todos esses anos até chegar ao nível de evolução que se encontram atualmente. As primeiras redes, que foram criadas entre meados da década de 60, eram especialmente utilizadas para transferências de dados de um computador para outro, partindo do ponto em que o armazenamento de dados era completamente externo, ou seja, a troca e armazenamento de informações eram feitos com cartões perfurados, estes suportavam apenas algumas poucas dezenas de caracteres (cerca de 80 caracteres por cartão, usando como exemplo o padrão IBM), que tornava a troca de dados, muito demorada, trabalhosa e ineficaz.

De acordo com Marimoto (2008), na transição da década de 60 para 70, foi criada a Arpanet, o embrião da Internet como é conhecida e usada atualmente. Uma rede que inicialmente continha apenas quatro nós, que interligados através de links de 50 kbps usando linhas telefônicas adaptadas para uso de dados, respondiam pelos nomes SRI, UTAH, UCSB e UCLA (*Stanford Research Institute*, Universidade de Utah, Universidade de Santa Barbara, Universidade da California, Universidade de Santa Barbara).

Por menor que pareça o link de conexão dessa rede (50 kilobits por segundo), era uma velocidade incrível naquela década, principalmente porque os modems da época transmitiam informações a apenas 110 bits por segundo, o que corresponde a 825 caracteres de texto por minuto.

Essa rede que foi utilizada com a finalidade de testes teve como propósito inicial interligar quatro computadores, cresceu rapidamente ao ponto de, em 1973, já interligava trinta instituições como universidades, órgãos militares e mesmo empresas, demonstrado na figura 1. No entanto para se manter uma constante conexão, cada nó era ligado a mais dois outros nós, ao menos que isso não existisse

[*]Discente da Faculdade de Tecnologia de Taquaritinga, phnahes@gmail.com
[**]Docente da Faculdade de Tecnologia de Taquaritinga, marcoaapereira@gmail.com

realmente a possibilidade desta ligação, devido a limitações físicas, tornando viável a existência da "estabilidade" na comunicação, mesmo que houvesse a interrupção de um ou vários links.

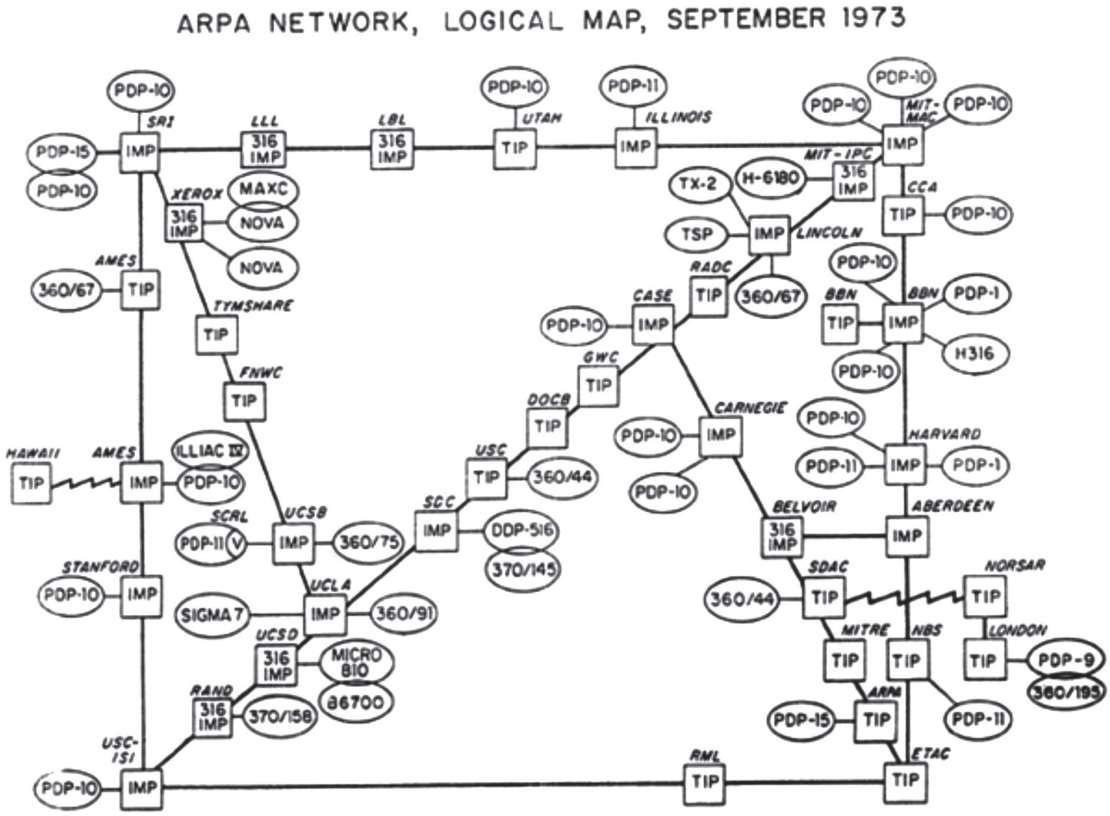

Figura 1: Diagrama da rede Arpanet em 1973
Fonte: Marimoto (2008)

Relata Marimoto (2008), com o surgimento do TCP/IP em 1974, este se tornou o protocolo padrão para a Arpanet e logo após para a atual Internet, tornando possível o desenvolvimento de recursos utilizados hoje, como TELNET (protocolo cliente-servidor que possibilita execução de instruções em um computador remoto), HTTP (protocolo usado para transferência de páginas multimídia pela internet), FTP (protocolo utilizado para transferência de arquivos entre computadores), entre outros, que permitem aos usuários trocarem informações e acessar outros computadores remotamente.

A complexidade da rede foi aumentando com o tempo devido ao crescente número de usuários, tornando praticamente impossível e inviável ter que lembrar o endereço IP de cada computador de cada instituição. A partir desta dificuldade em 1980 surge o DNS (*Domain Name System*), ou seja, um sistema que define nomes de domínios a computadores através de seu endereço IP (*Internet Protocol*).

Após muitos estudos, surge no Laboratório de desenvolvimento da Xerox o primeiro padrão Ethernet, este que transmitia a 2.94 megabits por cabos coaxiais e permitia a conexão de 256 estações de trabalho. Logo após com o passar dos anos, aparece seu sucessor, o padrão Ethernet, com velocidade de 10 megabits, ainda existente hoje em algumas instituições.

Inicialmente, porém, o padrão Ethernet e a Arpanet não tinha nenhuma ligação direta, pois redes Ethernet eram usadas para ligar estações de trabalho aos servidores das instituições, e a partir deles, usando cabos telefônicos para que houvesse a interligação com outras instituições através da Arpanet.

No início da década de 90, conforme Marimoto (2008), aplicações de tecnologias Ethernet em constante desenvolvimento, já transferia dados com uma taxa de transmissão de 100 megabits. O uso crescente da Arpanet, e o número de computadores pessoais aumentando, dá-se então a origem da Internet.

Mas ainda na década de 90, com a divulgação da Internet e abertura da mesma para qualquer usuário que tenha um computador, as redes se popularizam de maneira assustadora, tornando-se cada vez mais comum a sua utilização, e tomando outras dimensões. As redes são hoje, a melhor forma de reduzir custos de implantação e utilização de recursos, pois através delas podem ser compartilhados dispositivos como impressoras, alem de reduzir custos com a não utilização de dispositivos de mídia externo, devido a não ter necessidade dos mesmos para a transferência de dados entre estações de trabalho.

A partir deste ponto as redes começam a ser classificadas quanto à sua área de abrangência. São estas as classificações: WAN, Rede de Longa Distância, conectam computadores separados por grandes distâncias (superiores a centenas de quilômetros), utilizam redes de telefônica, satélite ou sistemas de fibra óptica, MAN, Rede de área Metropolitana, esta conecta computadores separados por distância média (cerca de dezenas de quilômetros), também utilizam sistemas de fibra óptica ou redes telefônicas, e por fim as LANs, Redes de Área Local, que conectam computadores a pequenas distâncias, como em escritórios, CPDs, entre outros exemplos.

Como relata USP (2009), em pesquisas, sem dúvida a evolução das redes de computadores e das telecomunicações é um caminho sem volta, ou seja, leva a uma convergência entre tecnologias, padrões, dispositivos e aplicações, onde a evolução, a preocupação com a consistência e a confiabilidade da informação torna-se algo inevitável.

SEGURANÇA EM REDES

Como afirma Pinheiro (2006), neste contexto, a evolução das redes de computadores, suas arquiteturas e seus processos são influenciados por uma nova realidade e uma gama de fatores relacionados com a disponibilidade e com a segurança da informação trocada, assumindo grande relevância.

Muito se tem visto sobre ataques de redes, exploração de vulnerabilidades de Sistemas Operacionais e aplicações para os mesmos, tornando necessário programar mecanismos de acessibilidade, segurança e de tolerância a falhas, capazes de garantir o acesso rápido e seguro às informações, independente da localização “geográfica” dentro da rede.

A partir deste ponto nos deparamos com diversos fatores que implicam na melhor segurança de uma interligação de computadores, como Firewalls, Proxys, e outras barreiras que impeçam o ataque a vulnerabilidades do sistema.

POLÍTICAS DE CONFIGURAÇÃO SEGURA

Toda política de segurança adotada em uma rede na visão de Pinheiro (2006), é o fator mais importante para proteger a organização, pois através de um conjunto de regras pré-estabelecidas, evita-se que ameaças quebrem uma ou mais propriedades fundamentais existentes no contexto de segurança da informação (confidencialidade, integridade e disponibilidade dos dados).

As políticas de segurança não atribuem métodos específicos de como manipular ou combater uma ameaça, porém definem responsabilidades, direitos, penalidades e punições às pessoas que não a seguem de maneira correta, pessoas essas, que lidam com as informações, por exemplo: usuários, administradores de redes, funcionários, gerentes, entre outros.

A partir do momento em que todas as políticas de segurança foram estabelecidas na rede, é preciso focar a preocupação na configuração correta dos componentes e sistemas que estarão compondo essa rede. A documentação de todo processo de instalação e configuração é um dos pontos primordiais para uma boa configuração e manutenção caso haja problemas.

PREPARANDO A INSTALAÇÃO

Um princípio básico e fator decisivo para evitar problemas futuros, na hora de instalar o sistema, é dividir o disco rígido (*Hard Disk*) em várias partições em vez de usar apenas uma única partição ocupando o disco inteiro. Isso é recomendável por diversas razões segundo CERT-BR (2003):

- Usuário pode encher uma partição com permissão de escrita, parando alguns serviços do sistema que a utiliza;
- Caso uma partição seja corrompida por alguma razão, as outras partições provavelmente não serão afetadas;
- O uso de várias partições geralmente facilita o procedimento de *backup* do sistema;
- Entre outros, como ganho de desempenho no caso de existir varias partições e muitos outros pontos positivos.

A partir daí, é extremamente interessante que a divisão por partições, levando em conta que cada sistema e utilidade do servidor teria uma configuração particular. Contudo é recomenda-se analisar áreas onde são armazenados itens como:

- *Logs*;
- Arquivos temporários;
- Filas de envio e recepção de *e-mails* (servidores SMTP);
- Filas de impressão (servidores de impressão);
- Repositórios de arquivos (servidores FTP);
- Páginas Web (servidores HTTP);
- Programas do sistema operacional;
- Dados dos usuários.

Nessa lista há algumas áreas em que se aplicam esta técnica, afirma CERT-BR (2003), devido a pertencerem a determinados serviços, assim como outras áreas que também possam merecer atenção

ao criar as partições.

SENHAS E SERVIÇOS NÃO UTILIZADOS

Ter uma senha segura e difícil de ser quebrada hoje é fundamental para manter confiabilidade e confidencialidade dos dados transmitidos na grande rede. Conforme CERT-BR (2003) e CSIRT (2006), sites especializados em segurança de computadores, para muitos usuários, a invasão de um sistema e a obtenção de senhas é causada por falhas de sistemas, porém segundo uma pesquisa do Grupo de Resposta a Incidentes de Segurança do POP-MG, 80% dos casos de invasão são causados por senhas mal-elaboradas. Sendo assim:

- Nunca usar nomes ou números que possam ser descobertos por estranhos (datas, telefones, placa de carro, RG).
- Também nunca usar palavras com significados em outros idiomas.
- Usar senhas com no mínimo seis caracteres, segundo a norma ISO 1779, recomenda-se o mínimo de oito caracteres.
- Nunca usar a mesma senha em locais distintos.
- Alterar as senhas a cada três meses.

Não deixando de lado a configuração do sistema, deve-se também desabilitar serviços que não estão sendo utilizados. Por exemplo: Serviço de envio de E-mail em um servidor dedicado a ser um Proxy, ou um sistema dedicado a servir páginas web, não tem a necessidade de um software servidor SMTP, ou mesmo as estações de trabalho precisarem de um servidor Web instalado. Sendo assim pode-se desabilitar todos os daemons (programa de computador que roda em background, em vez de ser controlado diretamente por um usuário) que não são utilizados e que são instalados por padrão em um sistema Linux.

Uma das coisas que ajudam a tornar o sistema menos vulnerável a falhas e ataques segundo CSIRT (2006), é a instalação mínima, onde não existem programas inúteis para seu propósito. No entanto, alguns administradores têm receio de instalar um componente no qual ele desconheça, com medo de perder alguma funcionalidade do sistema. Exatamente por isso, sistemas mais recentes vêm com um mecanismo de controle de dependências, que informam ao administrador quais partes aquele programa necessita para funcionar, podendo então deixar de instalar outros softwares inúteis para os fins da aplicação, sem comprometer o sistema instalado.

PREVENÇÃO CONTRA MAU USO DOS RECURSOS

Existem alguns recursos que se mal configurados, podem definitivamente arruinar um sistema, dando acesso a usuários externos de maneira ilícita.

Com a configuração incorreta destes recursos ou serviços, podendo ser acessados por pessoas externas à organização, pode-se de várias formas causar efeitos indesejáveis, como a utilização da CPU, da memória, dos discos, do link de acesso á internet da empresa. Podem ser usados por terceiros sem que exista pagamento por isso, e muitas vezes, estes recursos usados de tal forma que usuários legítimos do sistema não consigam utilizar o mesmo.

Um exemplo claro de má utilização por terceiros sobre recursos internos, são servidores Proxy que mal configurados ou sem atualizações de segurança, deixa então, que qualquer pessoa com conhecimentos suficientes reconheça o problema, e utilize de seus conhecimentos para se aproveitar da falha, transformando-a em um trampolim para uma futura invasão.

FIREWALL

Com uma definição básica e de acordo com CERT-BR (2003), Firewall define-se como equipamento ou dispositivo de rede que tem o objetivo de manter a segurança, aplicando políticas de segurança a um determinado ponto de controle de uma rede de computadores ou mesmo dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores. Os Firewalls consistem em controlar e regular o tráfego de dados na própria rede, ou em redes distintas, impedindo a transmissão ou recepção de acessos não permitidos de uma rede para outra.

O Firewall pode ser tanto lógico, ou seja, um software que dá funcionalidade de controle e filtro de tráfego a um computador, quanto físico, que são equipamentos de uso dedicado para filtragem de redes, instalados em pontos críticos de controle do tráfego. Ou mesmo a combinação de ambos, que ajuda a tornar a rede cada vez mais segura quanto complexa.

TIPOS DE FIREWALL

Atualmente existem quatro tipos básicos de firewalls, sendo eles, de acordo com (NED*,*1999)*:*

- Filtro de Pacotes, este que analisa individualmente os pacotes, na medida em que são transmitidos, verificando informações das camadas dois e três do modelo OSI.
- Filtro de Estados, que analisa e identifica o protocolo dos pacotes transitados para adivinhar as respostas. Resumindo, o Firewall guarda o estado de todas as últimas transações efetuadas e analisa, inspecionando o tráfego para evitar pacotes não legítimos.
- Firewall de Aplicação, esse trata dos pacotes vindos da última camada do modelo OSI (Camada de Aplicação), ou seja, instalado junto com a aplicação a ser protegida, ele analisa particularidades do protocolo utilizado e toma decisões que podem evitar ataques maliciosos à rede.
- IDS é sistema de detecção de intrusão, que tem como um objetivo principal detectar se existe alguém tentando invadir seu sistema ou se é apenas um usuário legítimo que está fazendo mau uso do mesmo. Esta ferramenta roda normalmente em *background* e só notifica quando detecta alguma atividade que seja suspeita ou ilegal.

MELHOR UTILIZAÇÃO DO FIREWALL

A localização de um sistema de Firewall dentro de uma rede depende particularmente das políticas de segurança, já estabelecidas anteriormente. Para cada caso, entretanto, existe um conjunto de regras que devem ser aplicadas, tais elas que (NED, *1999*):

- Todo fluxo de rede, ou seja, todo o tráfego deve passar pelo firewall, caso contrário, existindo rotas alternativas, pode comprometer a segurança da rede.
- Ter um Filtro de Pacotes no perímetro da rede, localizado entre o roteador as estações de trabalho,

ou mesmo na borda da rede interna com a externa, aumentando assim a proteção contra acessos indevidos e bloqueio global de tráfego indesejado.

- Colocar servidores com conteúdo WEB, o mais isolado possível dos outros computadores da rede, para que estes não fiquem vulneráveis à rede externa (Internet). Este conceito é conhecido como DMZ (*Desmilitarized Zone*, ou Zona Desmilitarizada).
- Utilizar Firewalls no contexto da rede interna, assim isolando redes separadas, e distintas, para que não exista colisão ou mesmo interceptação do tráfego entre elas.

CRITÉRIOS DE FILTRAGEM

Existem basicamente duas maneiras ou dois critérios de filtragem que podem ser empregados em um firewall (NED, *op. cit.*), sendo o primeiro *default deny*, ou seja, todo tráfego que não for explicitamente permitido é bloqueado. E o segundo *default allow,* todo tráfego que não for explicitamente proibido é liberado.

Porém a configuração dos firewalls deve seguir a configuração das políticas de segurança da rede a ser aplicada. Normalmente é utilizado com mais freqüência o *default deny* que exige uma interação bem mais ativa do administrador, que é obrigado a intervir de maneira explicita para liberar o tráfego desejado, evitando assim erros e falhas de segurança.

IMPLANTAÇÃO DE FIREWALLS

Como qualquer outro fator em uma rede, o Firewall também pode ser empregado e modelado dependentemente da sua estrutura de rede, incluindo fatores lógicos e físicos da mesma, dependendo de quanto a rede vai ser protegida dos custos, das funcionalidades pretendidas, entre muitos outros fatores como relata CERT-BR (2006).

Um exemplo simples da aplicação de um firewall ou está no seguinte caso demonstrado na figura 2:

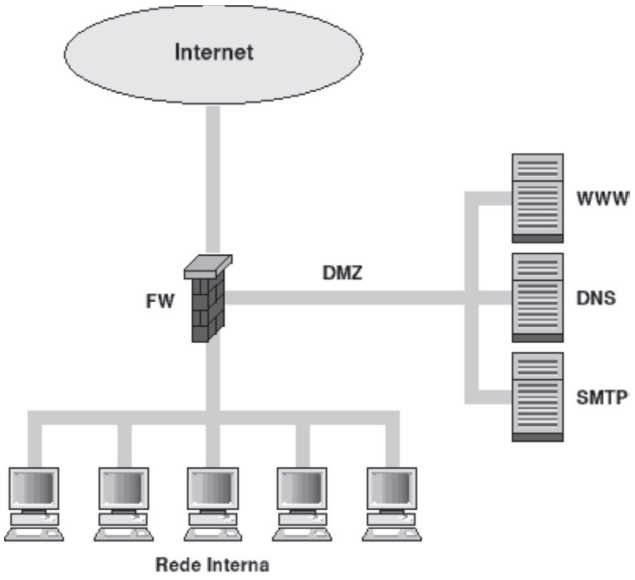

Figura 2: Exemplo simples de firewall
Fonte: CERT-BR (2009)

Utilizando este modelo como exemplo, pode-se demonstrar uma arquitetura funcional que pode eventualmente ser adotada em alguma situação real devido à simplicidade do modelo, porém não deixando de lado a possivel existência de algumas adaptações.

A figura 2 mostra um exemplo simples de uso do *firewall*. No exemplo, o computador do *firewall* contém três interfaces de rede: uma para a rede externa, uma para a rede interna e outra para a DMZ (*Desmilitarized Zone)*. Por padrão, este *firewall* bloqueia tudo, liberando apenas o que for explicitamente declarado em suas regras (*default deny*). O tipo de firewall recomendado a ser utilizado é o *stateful firewall*, que dinamicamente gera regras que permitem a entrada de respostas oriundas das conexões iniciadas na rede interna, no entanto, não é necessário incluir regras específicas e separadas para a entrada dessas respostas individualmente.

No exemplo acima, há o seguinte tráfego liberado:

- Interface Externa:
    - Saída: Libera saída de tudo com exceção dos
        - Pacotes com endereços de origem pertencentes a redes privadas;
        - Pacotes com endereços de origem pertecentes a blocos de rede interna;
    - Entrada: Libera entrada apenas aos pacotes que obedecem às seguintes combinações de protocolo, endereço e porta de destino:
        - Porta 25, Protocolo TCP, endereço do servidor SMTP;
        - Porta 53, Protocolo TCP e Porta 53, Protocolo UDP, endereço do servidor DNS;
        - Porta 80, Protocolo TCP, endereço do servidor WWW.
- Interface Interna:
    - Saída: Libera saída de tudo;
    - Entrada: Não Libera entrada de nada;
- Interface da DMZ:
    - Saída: Libera a saída das portas 25 no Protocolo TCP (Servidor SMTP), 53 Protocolo UDP e TCP (Servidor DNS) e 80 Protocolo TCP (Servidor WEB);
    - Entrada: além das mesmas regras de entrada da interface externa, também é permitido o tráfego para todos os servidores na porta de destino 22/TCP (SSH) e endereço de origem na rede interna.

Modelo adaptado de CERT-BR(2006)

Com essas políticas aplicadas, a segurança da rede se torna bem menos frágil a ataques, e são estas regras particulares de cada serviço e/ou recurso diponibilizado que torna ela inacessivel aos acessos externos e internos indevidos.

UTILIZAÇÃO DE LOGS

Segundo CERT-BR (2006), importantes para a administração segura de sistemas, eles registram as informações sobre funcionamento e erros, ou tentativas de acessos a setores e ambientes não permitidos por pessoas indevidas. São estes que em mãos competentes, como de administradores de redes, podem servir para aprimorar cada vez mais a segurança da rede.

Algumas práticas são recomendáveis quando o assunto é monitoramento de logs, sendo elas:

- Ter o hábito de analisar todos os logs;
- Fazer isso em períodos constantes, pelo menos uma vez por dia, dependendo da funcionalidade e nivel de risco daquele servidor;
- Identificar o padrão de comportamento normal dos seus sistemas, para que possa encontrar eventuais anomalias com maior rapidez, por já conhecer o sistema.

Contudo na maioria dos casos, relata CERT-BR (2006), é humanamente impossível analisar todos os logs, de diversos servidores. Para essa finalidade, foram criadas ferramentas de criação e monitoramento de logs, como o Nagios, para sistemas Linux.

CONCLUSÃO

Mesmo com muitas formas de quebrar a segurança de uma rede, desde o começo da tecnologia para compartilhamento de dados, os técnicos e engenheiros vêm procurando e criando ferramentas e técnicas para proteger as redes. Sendo assim, mesmo não sendo completamente seguras, muito se tem feito para que esse fim seja alcançado, desde sistemas complexos de firewall e técnicas de particionamento até análises de log e utilização de recursos da própria máquina.

ABSTRACT

This paper approaches the networks appearing and their evolution. It also approaches a set of information and techniques regarding to network security, where shared information could be caught, if vulnerabilities are not solved.

KEYWORDS: *Network. Security. Configuration. Evolution. Firewall.*

REFERÊNCIAS

CERT. BR. *Práticas de Segurança para Administradores de Redes Internet.* http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html, 2003.

CSIRT POP-MG. *Como criar boas senhas*. http://www.csirt.pop-mg.rnp.br/docs/senhas.pdf, 2006.

MARIMOTO, C. *História das redes.* http://www.guiadohardware.net/tutoriais/historia-redes, 2008.

NED, F. *Ferramentas de IDS,* http://www.rnp.br/newsgen/9909/ids.html, 1999.

PINHEIRO, J. M. S. *A Evolução da Revolução.* http://www.projetoderedes.com.br/artigos/artivo_evolucao_da_revolucao.php, 2005.

PINHEIRO, J. M. S. *Introdução às supervisões e Controle.* http://www.projetoderedes.com.br/artigos/artigo_redes_de_supervisao_e_controle.php, 2006.

USP. *Segurança de redes,* http://www.ime.usp.br/, 2009.