Curso de Tecnologia em Redes de Computadores
Disciplina: Auditoria e Análise de Segurança da Informação - 4º período
Professor: José Maurício S. Pinheiro

AULA 2: Segurança Física e Segurança Lógica

Segurança Física e Lógica em Redes de Computadores

"A estratégia vencedora de negócios consiste em operações focadas no mercado, e suportadas por uma TI/SI - Tecnologias e Sistemas de Informação que funcione com a máxima eficiência".

Uma instalação de rede, bem planejada e implementada, garante a empresa que seus Sistemas de Informação estarão muito mais tempo em funcionamento, evitando perdas de produtividade e lucratividade. Portanto, aspectos de seguranças física e lógica devem ser observados e constantemente avaliados, para suportar os negócios da empresa.

A implementação de segurança em redes de computadores deve ocorrer sob dois aspectos:

- **Segurança Física.**
- **Segurança Lógica.**

Segurança Física

A segurança física é o primeiro aspecto que deve ser considerado no que se refere à proteção do hardware de redes de computadores, tendo em vista a proteção de dados e informações. O nível de segurança física dependerá**:**

- Do tamanho da empresa;
- Da importância dos dados;
- Dos recursos disponíveis para implementação da segurança.

A segurança física deverá contemplar:

- **Acesso às instalações da empresa:**
  - Controle de veículos e pessoas;
  - Controle de pessoas na área de Informática, com registros de acessos, escritos ou em fitas;
  - Utilização de equipamentos e Tecnologias de segurança de acesso a áreas restritas.

- **Sistemas elétricos:**
  - Sistema de aterramento eficiente;
  - Rede elétrica estabilizada e específica para equipamentos críticos de informática;
  - Utilização de equipamentos do tipo "No-Break" ou UPS;

  - Cabeamento elétrico separado do cabeamento de redes de computadores e telefonia;
  - Utilização de protetores contra surtos elétricos e ruídos.

- **Sistemas contra incêndios:**
  - Cofres e salas especiais para armazenar arquivos e equipamentos críticos de informática;
  - Identificação e manutenção dos equipamentos contra incêndio;
  - Sinalização para localização dos equipamentos contra incêndio;
  - Equipe treinada para situações de emergência.

- **Proteção dos cabos de rede:**
  - Utilizar cabeamento e conectores padrão de boa qualidade;
  - Utilizar protetores adequados para linhas de transmissão de dados e de telefonia;
  - Utilizar cabeamento estruturado;
  - Identificar os cabos críticos, principalmente Backbones de Fibras óticas.

- **Proteção de servidores e redes:**
  - Instalação de Servidores em salas apropriadas, longe de condições climáticas e ambientais que possam danificá-las e com restrição de acessos;
  - Instalação de Firewall (Hardware) nos pontos de conexão externa da rede.

Segurança Lógica

A segurança lógica é um conjunto de meios e procedimentos para preservar integridade e controle de acesso às informações e recursos contidos nos servidores e computadores centrais, sejam os mesmos armazenados em fitas ou discos, de forma que não sejam manipulados por pessoas não autorizadas. A segurança lógica deverá contemplar:

- **Acesso aos recursos:**
  - Compartilhamento protegido por Senhas;
  - Controle das permissões de acesso a nível individual e de grupo, através de Contas e Senhas;
  - Certificação Digital.
  - Firewall (Software) – Proxy Server.

- **Acesso aos arquivos:**
  - Implementação e manutenção de software Antivírus;
  - Criptografia;
  - Assinaturas digitais;
  - Controle de permissões em nível de informação;

- SGBD de boa qualidade.

- **Proteção dos dados:**
  - Rotinas de BACKUP / RESTORE eficientes, com log das atividades do backup;
  - Utilização modernas mídias de armazenamento (DAT, DDS, Mídias Ópticas, etc.);
  - Renovar constantemente as mídias de Backup;
  - Manter as mídias onde estão os Backups fora da área de Informática e, preferencialmente mantê-las em cofre contra incêndios;
  - Contratação Serviços Storage remoto (Backup através de VPN);
  - Sistema de tolerância à falhas.

Esses sistemas protegem os dados, duplicando-os e colocando-os em diferentes fontes físicas, tais como: diferentes partições ou discos. Ambientes com Sistemas tolerantes a falha nunca devem substituir um bom sistema de *Backup*.

Sistemas de Proteção e Prevenção de Intrusão

A segurança deve ser uma preocupação básica ao se elaborar o projeto de uma rede de computadores. Normalmente a segurança é inversamente proporcional à simplicidade e facilidade de uso / configuração da rede. Por exemplo, um servidor da rede pode centralizar diversos serviços para atender a rede externa (Internet) e a rede privada (interna). Esta configuração gera problemas de segurança como:

- **Exposição da rede interna à Internet** - Os serviços da rede interna (e-mail, por exemplo) estando localizados na mesma máquina que provê os serviços externos (web, por exemplo), deixarão os dados do usuário expostos em caso de uma invasão;
- **Maior fragilidade a vulnerabilidades** - O fato de concentrar muitos serviços em uma única máquina gera esse tipo de problema, pois quanto mais serviços disponíveis, mais vulnerabilidades podem ser exploradas e, conseqüentemente, existe um maior grau de exposição e risco de invasão;

Opção pelo firewall

O Firewall opera nas camadas de transporte e de rede do modelo TCP/IP, tendo como principal finalidade a filtragem de pacotes. Ele analisa todos os pacotes que entram ou saem de todas as interfaces de rede a ele conectadas, ou seja, tanto pacotes destinados diretamente ao Firewall, quanto destinados a qualquer host conectado a ele por meio de alguma de suas interfaces de rede. Sua principal função também é bloquear todas as portas quem não estejam sendo utilizadas.

Um firewall é uma passagem (“gateway”) que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a Internet. O firewall pode também estabelecer passagens seguras entre redes internas. Implantar um firewall, com regras rígidas de segurança e que não permita que as máquinas da rede sejam acessadas por máquinas remotas é uma grande conquista em termos de segurança.

Por vezes, algumas máquinas da rede precisam receber acessos externos, é o caso de servidores SMTP e servidores Web, por exemplo. Para permitir que estas máquinas possam desempenhar suas funções, mas que ao mesmo tempo o restante da rede continue protegida, muitos firewalls oferecem a opção de criar uma zona onde essa vigilância é mais fraca conhecida como DMZ. Nesse caso, o controle de acesso a Internet pode ser feito através de um projeto de DMZ permitindo que todo o tráfego entre os servidores da empresa, a rede interna e a Internet passe por um firewall e pelas regras de segurança criadas para a proteção da rede interna.

Assim, o firewall se torna um único ponto de acesso à rede em que o tráfego poderá ser analisado e controlado por meio de scripts no firewall que definem o aplicativo, o endereço e os parâmetros de usuário. Esses scripts ajudam a proteger os caminhos de conectividade para redes e centros de dados externos.

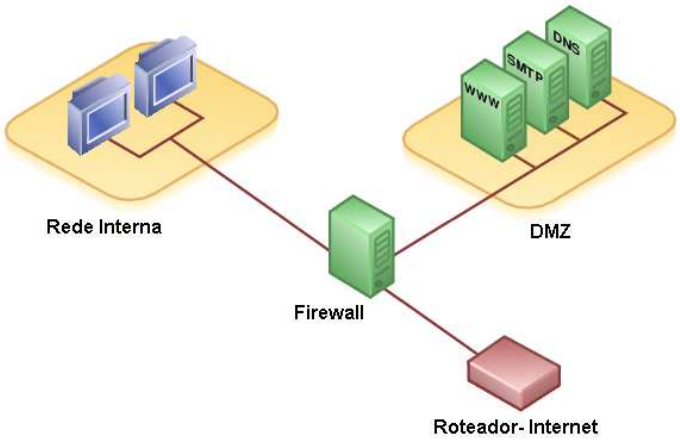

Figura 1 - Rede com firewall e DMZ

Rede de Perímetro

O termo rede de perímetro refere-se a um segmento de rede isolado no ponto em que uma rede corporativa alcança a Internet. As redes de perímetro destinam-se a criar um limite que permite a separação do tráfego entre redes internas e externas. Com este limite, é possível categorizar, colocar em quarentena e controlar o tráfego da rede de uma empresa. A segurança de perímetro é proporcionada por um dispositivo de perímetro, como um firewall, por exemplo, que inspeciona os pacotes e as sessões para determinar se devem ser transmitidos para a rede protegida ou a partir dela ou ser abandonados.

Os serviços e servidores que devem interagir com a Internet externa desprotegida são colocados na rede de perímetro (conhecida como zona

desmilitarizada) e na sub-rede filtrada. Isto ocorre para que, caso invasores consigam explorar vulnerabilidades em serviços expostos, possam avançar apenas uma etapa no acesso à rede interna confiável.

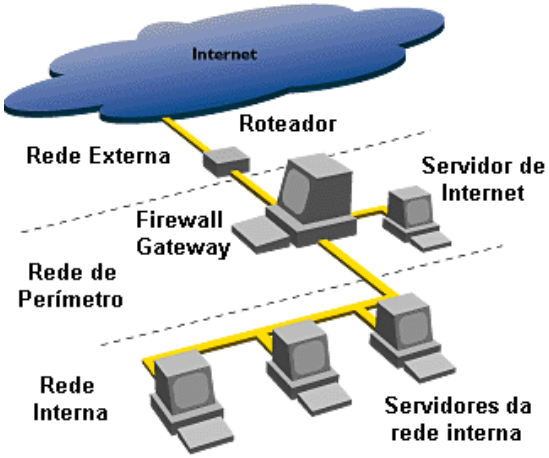

Figura 2 - Rede de perímetro

Zona Desmilitarizada – DMZ

Uma DMZ ou ainda "Zona Neutra" corresponde ao segmento ou segmentos de rede, parcialmente protegido, que se localiza entre redes protegidas e redes desprotegidas e que contém todos os serviços e informações para clientes ou públicos. A DMZ pode também incluir regras de acesso específico e sistemas de defesa de perímetro para que simule uma rede protegida e induzindo os possíveis invasores para armadilhas virtuais de modo a se tentar localizar a origem do ataque.

Podemos ter dois tipos de DMZ's: a interna, só acessada pelo usuário da rede interna e a DMZ externa, acessada por qualquer usuário da Internet. Este conceito aliado ao de VLAN's também permite a implantação de DMZ's privadas, ou seja, a possibilidade de DMZ's específicas para cada cliente de hosting ou para a hospedagem de servidores.

As DMZ's são sub-redes onde se hospedam os servidores/serviços de um provedor, protegidos contra ataques da Internet por um firewall. Em geral é necessário especificar uma faixa de endereços IP, ou informar diretamente os endereços das máquinas que devem ser incluídas nessa zona.

Implantação da DMZ

O projeto lógico de uma rede que visa conexões com a Internet deve envolver a criação de uma DMZ. Esta DMZ será protegida por um sistema de defesa de perímetro, onde os usuários de Internet podem entrar livremente para acessar os servidores web públicos, enquanto que os dispositivos localizados nos pontos de acesso (firewall, switch e servidor de perímetro) filtram todo o trafego não permitido, como por exemplo, pacotes de dados que tentam prejudicar o funcionamento do sistema. Ao mesmo tempo a rede interna privada esta protegida por outro firewall.

A zona desmilitarizada comporta-se como uma outra sub-rede, atrás de um firewall, onde temos uma máquina segura na rede externa que não executa nenhum serviço, mas apenas avalia as requisições feitas a ela e encaminha cada serviço para a máquina destino na rede interna.

No caso de uma invasão de primeiro nível, o atacante terá acesso apenas ao firewall, não causando problema algum para a rede da empresa. Já em invasões de segundo nível, o atacante conseguirá passar do firewall para a sub-rede interna, mas ficará preso na máquina do serviço que ele explorar.

Em todos os casos, devem-se analisar com cuidado quais serviços podem ser colocados dentro da DMZ. Por exemplo, na maioria das situações, o servidor de e-mail é inserido na DMZ. Nesse caso, em uma invasão ao servidor de e-mail, os únicos dados que poderão ser comprometidos são os e-mails e mais nenhum outro. Já a colocação de um servidor de DNS em uma DMZ não é recomendável para a segurança da rede. Como uma DMZ permite acesso menos seguro para alguns segmentos da rede, a colocação desse servidor nesta situação poderia comprometer a segurança dos endereços de todos os servidores da rede local e roteadores.

Convém salientar que durante a elaboração do projeto da rede, é recomendável se manter os serviços separados uns dos outros. Assim, será possível adotar as medidas de segurança mais adequadas para cada serviço.

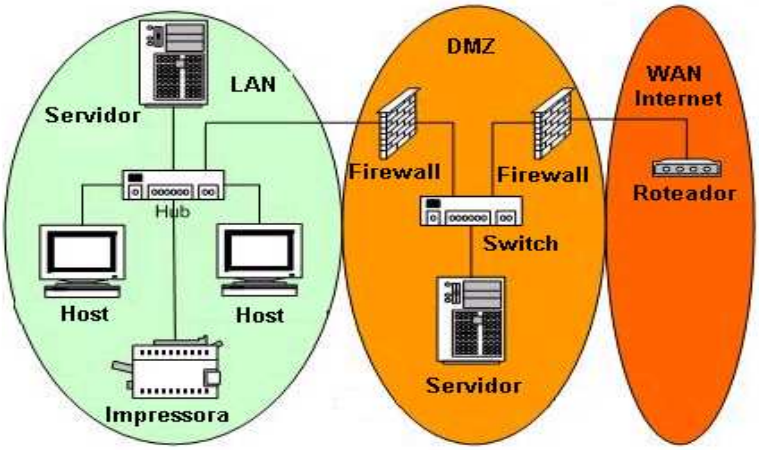

Figura 3 - Exemplo de rede com DMZ

IDS (Intrusion Detection System)

Uma infra-estrutura de segurança de redes mais simples consiste em um firewall implementado no perímetro. Isso funciona bem quando há uma interação limitada entre as redes externas e internas, quando os usuários internos são confiáveis e quando o valor das informações na rede é limitado. Entretanto, os aplicativos na rede e a interação entre redes aumentaram significativamente, o nível de confiança nos usuários internos diminuiu consideravelmente e o acesso vem se estendendo a um público maior, incluindo parceiros e funcionários temporários. Os agressores e suas ferramentas estão muito mais sofisticados. E, o mais perigoso, as informações disponíveis em rede se tornaram ainda mais cruciais para a execução de negócios.

Recentemente, várias empresas passaram a aumentar suas infra-estruturas de segurança para acomodar essas mudanças. Através de sistemas de detecção de vírus, verificadores de vulnerabilidades, codificação e sistemas de detecção de intrusões (IDS), as empresas vêm se esforçando para detectar e prevenir ameaças à segurança de suas redes. Todas essas tecnologias apresentam complexidades e dificuldades, mas principalmente os sistemas de detecção de intrusões enfrentam desafios complexos.

Considerado freqüentemente como uma das principais linhas de defesa contra agressores, a detecção de intrusões se tornou rapidamente um componente crucial de um bom sistema de defesa. Eles são desenvolvidos baseando-se nos tipos conhecidos de ataques e também verificando alterações de comportamento do tráfego da rede. Sempre que é detectada alguma alteração no comportamento do tráfego ou identificando algum tipo de ataque, ele pode enviar algum tipo de alerta aos administradores da rede, contra-atacar ou simplesmente se defender baseado em alguma configuração pré-definida.

Detecção de Anomalias na Rede

Uma anomalia é definida como algo diferente, anormal, peculiar ou que não seja facilmente classificado. Apesar desse conceito se aplicar a praticamente tudo, estamos interessados em como se aplica à segurança de computadores. Neste contexto, uma anomalia pode ser definida como ações ou dados que não sejam considerados normais por um determinado sistema, usuário ou rede.

Essa definição abrange ainda uma grande variedade de itens e pode incluir tópicos como padrões de tráfego, atividades dos usuários e comportamento de aplicativos. Acredita-se que pelo menos uma significativa porção das ameaças ou condições que causem alarme deve manifestar-se como anomalias, sendo assim detectáveis.

A maioria dos sistemas de detecção de anomalias que se concentram em segurança normalmente se enquadra em três categorias gerais: comportamental, padrão de tráfego ou protocolo.

Os sistemas que procuram por anomalias em padrões de comportamentos (normalmente o comportamento de usuários) são considerados sistemas de anomalias comportamentais. Esses sistemas são

normalmente de características, porém eles podem abranger também alguns critérios de estatísticas, como os tipos de aplicativos e protocolos usados em várias horas do dia, a relação entre a origem e o destino das atividades da rede ou até mesmo os tipos de anexos de e-mail que são enviados através de um sistema.

Os sistemas que procuram por anomalias em padrões de tráfego da rede são considerados sistemas de anomalias no padrão de tráfego. Esses normalmente são de natureza estatística, apesar de incluírem algumas características como volume de tráfego, mistura de protocolos e várias distribuições na origem e no destino. Para ilustrar, considere algum gerenciamento de rede ou sistemas simples de monitoração de negação de serviços, que possuem a vantagem de operar em um domínio muito maior e variado, e que podem ser criados a partir de um número de bons modelos de estatísticas. Porém, a desvantagem é que esses sistemas freqüentemente não são capazes de detectar a maioria das anomalias qualitativas ou quantitativas sutis. Eles apresentam também algumas dificuldades na definição de uma base confiável para o desempenho da análise de estatísticas.

Os sistemas que procuram por anomalias em protocolos são considerados sistemas de anomalias de protocolos. Normalmente sistemas de características, esses tendem a variar um pouco de acordo com a implementação, mas os mais eficientes são freqüentemente implementados como sistemas de modelo rígido. Esse tipo de sistema tira proveito do fato de que os protocolos sozinhos são geralmente muito restritos. Eles tendem a limitar muito a natureza e ordem das transações e são geralmente muito bem descritos por alguma implementação ou documento de referência. Sendo assim, é possível construir um modelo bastante rígido do que deve ocorrer e qualquer divergência desse modelo pode ser facilmente observada. Outra vantagem desse sistema é que ele pode detectar uma grande variedade de anomalias dentro do espaço do protocolo, e pode ser construído com muita eficiência. A desvantagem, porém, é que pode ser difícil de estimar o efeito da anomalia observada de forma acurada, e que alguns tipos de transações de protocolo problemáticas (como ataques, por exemplo) não se manifestam como anomalias.

Segurança Integrada

Esse método de segurança combina várias tecnologias de segurança com compatibilidade de política, gerenciamento, serviço e suporte, e pesquisa avançada para a proteção completa. Através da combinação de várias funções, a segurança integrada pode proteger com mais eficiência contra uma variedade de ameaças em cada nível para minimizar os efeitos dos ataques de rede.

As tecnologias de segurança principais que podem ser integradas incluem:

- **Firewall** - Controla todo o tráfego de rede através da verificação das informações que entram e saem da rede (ou parte dela) para ajudar a garantir que nenhum acesso não autorizado ocorra;

- **Detecção de Intrusão** - Detecta o acesso não autorizado e fornece diferentes alertas e relatórios que podem ser analisados para políticas e planejamento da segurança;
- **Filtragem de Conteúdo** - Identifica e elimina o tráfego não desejado de informação;
- **Redes Privadas Virtuais (VPN)** - Assegura as conexões além do perímetro, permitindo que organizações se comuniquem com segurança com outras redes através da Internet;
- **Gerenciamento de Vulnerabilidade -** Permite a avaliação da posição de segurança da rede descobrindo falhas de segurança e sugerindo melhorias;
- **Proteção com Programas Antivírus** - Protege contra vírus, worms, Cavalos de Tróia e outras pragas virtuais.

Individualmente, essas tecnologias de segurança podem ser incômodas para instalar e geralmente são difíceis e caras de gerenciar e atualizar. Entretanto, quando integradas em uma solução única, elas oferecem uma proteção mais completa enquanto a complexidade e o custo são reduzidos.