Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar

Threats and Attacks to Information Systems: prevent and antecipate

José Maurício dos Santos Pinheiro [1]

Artigo Original

Original Paper

Palavras-chaves:

Ameaça

Ataque

Vulnerabilidade

Proteção

Segurança

Resumo

A segurança dos sistemas de informação configura-se paradoxalmente como um custo e uma necessidade para a sobrevivência de uma corporação. Se, por um lado, obter um sistema com maior segurança raramente é visto como algo de valor significativo, por outro, o perigo de um ataque não é ignorado totalmente. Neste contexto, a segurança computacional deve ser tomada como opção estratégica e não apenas tecnológica ou gerencial, com impacto positivo e inegável sobre o negócio, estando relacionada ao conjunto das medidas que visam dotar as redes de computadores com capacidade de inspeção, detecção, reação e reflexo aos potenciais ataques, permitindo reduzir e limitar as vulnerabilidades e o impacto das ameaças quando estas se concretizam. Com esse objetivo são utilizados sistemas de detecção de intrusões (Intrusion Detection Systems - IDS), sistemas automáticos, que funcionam em tempo real, capazes de analisar o tráfego de uma rede de comunicação de acordo com uma série de funções que, de modo integrado, são capazes de detectar, analisar e responder a atividades suspeitas na rede.

Key words:

Threat

Attack

Vulnerability

Protection

Security

Abstract

The information systems security is paradoxically configured as a cost and a necessity for a corporation survival. If, on the one hand, obtaining a system with a bigger security is rarely seen as something with a significant value, on the other hand, the risk of an attack is not totally ignored. In this context, the computational security must be taken as an strategic option and not only a technological or management one, with a positive and non-denied impact under the business, and the computation security being related to all the actions which aim to give the computers net the capacity of inspection, detection, reaction and reflex of potential attacks, allowing reduce and limit the vulnerabilities and the threats impact when these ones come true. With that objective, intrusion detections systems are used, automatic systems which work in real time, able to analyze the traffic in a communication net according to a series of functions which, in an integrated way, are able to detect, analyze and answer to suspicious activities in the net.

1. Introdução

A comunicação sempre foi uma das maiores necessidades da sociedade humana. De acordo com o crescimento das civilizações, que ocupavam áreas cada vez mais dispersas geograficamente, a comunicação a longa distância se tornava uma necessidade cada vez maior e um desafio. Formas de comunicação rudimentares como sinais de fumaça ou pombos-correio foram algumas das maneiras encontradas por nossos ancestrais para tentar aproximar as comunidades distantes. A invenção do telégrafo por Samuel Morse em 1838, inaugurou uma revolução no tratamento das informações. Equipamentos para processamento e armazenamento de

[1] Especialista - Curso Tecnológico de Redes de Computadores - UniFOA

dados foram alvo de grandes investimentos e, a introdução das redes de computadores nos meios acadêmicos e industriais na década de 1950 foi, provavelmente, o maior avanço neste sentido.

As redes de computadores sofreram mudanças para atender à evolução das aplicações, que passaram de sistemas isolados (stand-alone) e fechados, sobre os quais as organizações detinham total controle, para sistemas abertos e distribuídos, baseados em componentes off-the-shelf, dos quais as organizações têm um conhecimento e controle limitados. Atualmente, na quase totalidade dos casos, os sistemas de informação são escolhidos segundo as funcionalidades oferecidas e o investimento inicial, em detrimento da robustez, maturidade e do retorno do investimento a longo prazo ou benefícios indiretos.

Mitnick e Simon (2003, p. 4) enfatizam:

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano.

Esse fato é agravado pela visão limitada, ainda encontrada nas administrações que encaram a segurança da informação como custos, não envolvendo as demais áreas de negócio na análise dos problemas corporativos, limitando-se ao pagamento das "despesas com segurança" e não treinando adequadamente o pessoal envolvido com a utilização desses sistemas.

É importante salientar que a segurança da informação, mais que um problema de utilização de tecnologias, deve ser encarada como a gestão inteligente da informação, priorizando recursos e focando os investimentos no ambiente em que está inserida.

2. Ameaças e ataques

Uma ameaça consiste em uma possível violação de um sistema computacional e pode ser acidental ou intencional. Uma ameaça acidental é aquela que não foi planejada. Pode ser, por exemplo, uma falha no hardware ou no software. Já uma ameaça intencional, como o nome diz, está associada à intencionalidade premeditada. Pode ser desde um monitoramento não autorizado do sistema até ataques sofisticados, como aqueles realizados pelos hackers.

Algumas das principais ameaças aos sistemas nas redes de computadores envolvem destruição de informações ou recursos, modificação ou deturpação da informação, roubo, remoção ou perda de informação, revelação de informações confidenciais ou não, chegando até a paralisação dos serviços de rede.

Um ataque ocorre quando uma ameaça intencional é realizada. Os ataques ocorrem por motivos diversos. Variam desde a pura curiosidade, passando pelo interesse em adquirir maior conhecimento sobre os sistemas, até o extremo, envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de um governo ou uma determinada empresa ou serviço. Quando isso acontece, a notícia da invasão é proporcional à fama de quem a sofreu e normalmente representa um desastre em termos de repercussão pública.

São três os aspectos básicos que um sistema de segurança da informação deve atender para evitar a concretização das ameaças e ataques: Prevenção, Detecção e Recuperação.

2.1. Prevenção

- **Proteção de hardware:** normalmente chamada de segurança física, impede acessos físicos não autorizados à infra-estrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos quando se está fisicamente no local;
- **Proteção de arquivos e dados:** proporcionada pela autenticação, controle de acesso e sistemas antivírus. No processo de autenticação, é verificada a identidade do usuário; o controle de acesso disponibiliza apenas as transações pertinentes ao usuário e os programas antivírus garantem a proteção do sistema contra programas maliciosos;
- **Proteção de perímetro:** ferramentas de firewall e routers cuidam desse aspecto, mantendo a rede protegida contra tentativas de intrusão (interna e externa à rede).

2.2. Detecção

- **Alertas:** sistemas de detecção de intrusões alertam os responsáveis pela segurança sobre qualquer sinal de invasão ou mudança

suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, mensagem no console de gerência, celular, etc.;

• **Auditoria:** periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários inativos, etc.

2.3. Recuperação

• **Cópia de segurança dos dados (Backup):** manter sempre atualizados e testados os arquivos de segurança em mídia confiável e separados física e logicamente dos servidores;

• **Aplicativos de Backup:** ferramentas que proporcionam a recuperação rápida e confiável dos dados atualizados em caso da perda das informações originais do sistema;

• **Backup do Hardware:** a existência de hardware reserva, fornecimento autônomo de energia, linhas de dados redundantes, etc., podem ser justificados levando-se em conta o custo da indisponibilidade dos sistemas.

3. Princípios de Prevenção e Proteção

As informações podem ser classificadas de acordo com o eventual impacto gerado decorrente de acesso, divulgação ou conhecimento não autorizado. Logo, a segurança de uma rede de computadores está relacionada à necessidade de proteção dessas informações contra acessos não autorizados ou contra a utilização indevida dos recursos computacionais, além de preservar a integridade dos dados armazenados contra a manipulação de qualquer natureza.

As formas de proteção da informação devem ser definidas a partir da análise das possíveis ameaças e riscos que a rede está submetida, com a finalidade de manter sua confidencialidade, disponibilidade e integridade, e também para atender aos objetivos de gestão traçados pela alta direção.

Silva, Carvalho e Torres (2003, p. 17) afirmam:

> A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a autenticidade e o não repúdio.

As medidas de segurança podem ser classificadas, em função do modo como abordam as ameaças, em duas grandes categorias: prevenção e proteção. A prevenção é o conjunto das medidas que visam reduzir a probabilidade de concretização das ameaças existentes. Essas medidas, independentemente do seu objetivo, necessitam ser implementadas antes da concretização da ameaça, ou seja, antes do incidente ocorrer. O efeito das medidas de prevenção extingue-se quando uma ameaça se transforma num ataque.

As medidas de proteção tem como objetivo dotar os sistemas de informação com ferramentas capazes de garantir a integridade da rede frente a um ataque, bloqueando acessos indevidos e, até mesmo, respondendo instantaneamente às tentativas de intrusão.

4. Sistemas de Detecção de Intrusões

A segurança é um processo complexo, com componentes tecnológicos e humanos, envolvendo metodologias e comportamentos. Neste contexto, uma infra-estrutura de segurança mais simples consiste em um firewall implementado no perímetro da rede local de computadores (LAN). Esta estrutura funciona bem quando há uma interação limitada entre as redes externa e interna, quando os usuários internos são confiáveis e quando o valor das informações na rede é limitado (Fig.1).

Entretanto, os aplicativos usados na rede e a interação entre redes aumentaram significativamente, o nível de confiança nos usuários internos diminuiu consideravelmente e o acesso aos recursos da rede 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 continuidade dos negócios.

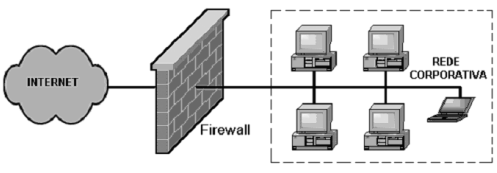

Figura 1 - Firewall implementado no perímetro da rede local

Os sistemas de detecção de intrusões (Intrusion Detection Systems - IDS), são sistemas automáticos que funcionam como verdadeiros sniffers e, em tempo real, analisam o tráfego na rede e detectam tentativas não autorizadas de acesso à infra-estrutura lógica. O grande objetivo destes sistemas é proporcionar uma reação efetiva aos ataques que um segmento de rede possa vir a sofrer.

Considerados freqüentemente como uma das principais linhas de defesa contra agressores, os IDS se tornaram rapidamente componente crucial para um bom sistema de defesa em rede. Eles atuam baseando-se nos tipos conhecidos de ataques e também verificando alterações de comportamento no tráfego de dados. Sempre que é detectada alguma alteração no comportamento desse tráfego ou identificado algum padrão de ataque, o sistema pode enviar um alerta aos administradores da rede, contra-atacar ou simplesmente se defender baseado em alguma configuração predefinida.

Segundo Nakamura e Geus (2007, p. 264):

> O sistema de detecção de intrusão (Intrusion Detection System – IDS) é um componente essencial em um ambiente cooperativo. Sua capacidade de detectar diversos ataques e intrusões auxilia na proteção do ambiente, e sua localização é um dos pontos a serem definidos com cuidado.

Uma organização que possua firewalls e routers, devidamente configurados, poderá evitar a grande maioria dos ataques contra seus sistemas. Porém, esta estrutura não possui qualquer tipo de conhecimento sobre o que acontece do lado de fora do seu perímetro, desconhecendo as tentativas de intrusão oriundas do exterior. Por outro lado, um IDS não oferece apenas visibilidade ao que acontece no exterior do perímetro lógico da rede ao detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto, não podem ser protegidas pelo firewall, mas revela igualmente o que acontece no seu interior: tentativas de acesso a servidores protegidos a partir da rede interna. “Um IDS não utiliza medidas preventivas, quando um ataque é descoberto age como um informante” (LAUREANO, 2002, P.6).

4.1. Tipos de IDS

Quanto ao tipo, os IDS atualmente disponíveis podem ser divididos em dois grandes grupos: baseados em host (Host-based Intrusion Detection Systems – HIDS) e baseados em rede (Network-based Intrusion Detection Systems - NIDS). Muitos dos sistemas existentes no mercado combinam estas duas formas de proteção, conseguindo deste modo uma visão muito mais abrangente da atividade dos sistemas de informação, são os IDS híbridos (Hybrid IDS), que aproveitam as melhores características do HIDS e do NIDS.

Tecnicamente, a combinação dos diferentes tipos de IDS proporciona uma proteção mais eficiente dos sistemas de informação contra ataques realizados internamente, bem como daqueles oriundos da Internet.

4.1.1. HIDS

Os sistemas baseados em host (HIDS) são programas dedicados a sistemas individuais, afinados às suas características e que detectam sinais de intrusão nas comunicações (de entrada ou de saída) dos sistemas que protegem. Esses sistemas fazem o monitoramento da rede com base em informações de arquivos de logs ou de agentes de auditoria.

No caso de se tratar de um servidor de banco de dados, por exemplo, o HIDS poderá analisar, além das transações do sistema operacional e do protocolo de comunicação, operações específicas dos aplicativos em utilização.

4.1.2. NIDS

Os sistemas baseados em rede (NIDS) monitoram o tráfego do segmento da rede em tempo real, com a interface de rede atuando em modo promíscuo. Desse modo é possível capturar os pacotes referentes ao ataque, analisar e responder praticamente ao mesmo tempo em que o segmento da rede é atacado.

Os NIDS podem ser divididos em duas partes que atuam em conjunto: sensores (ou sondas) e um gerenciador (ou console).

· Os sensores são colocados em pontos estratégicos da infra-estrutura, analisando todo o tráfego do segmento de rede onde estão inseridos, comparando-o com uma base de dados de padrões e assinaturas de ataques para identificar atividades suspeitas. A detecção é realizada pela captura e análise dos cabeçalhos

e conteúdos dos pacotes, que são comparados com esses padrões e assinaturas;

· O gerenciador é responsável pela administração integrada dos sensores, com a definição dos tipos de resposta a serem utilizados para cada evento de comportamento suspeito detectado. A comunicação entre gerenciador e sensores utiliza na maioria das vezes criptografia assimétrica para a formação de um canal seguro.

4.1.3. Sistemas Híbridos

Um sistema IDS híbrido tem como objetivo combinar as vantagens do HIDS e do NIDS, a fim de proporcionar uma melhor capacidade de detecção de intrusões. O IDS híbrido funciona como o NIDS coletando o tráfego de pacotes da rede, processando as informações e detectando e respondendo a ataques do mesmo modo como ocorre no HIDS.

Com relação ao gerenciamento, alguns sistemas podem ter uma centralização dos IDS, pois alguns sensores, baseados em rede, são localizados em diversos segmentos de rede e outros IDS, baseados em host, são usados em servidores. O gerenciador pode controlar as regras dos dois tipos, formando o IDS híbrido.

De acordo com Strebe e Perkins (2002, p. 288, tradução nossa):

> Sistemas IDS sempre requerem recursos da rede para funcionarem corretamente. Sistemas NIDS usualmente funcionam em firewalls ou computadores dedicados; isso normalmente não é problema porque esses recursos são disponíveis. Entretanto, Sistemas HIDS destinados a proteger servidores podem ter sérias restrições para funcionamento.

No caso dos servidores da zona neutra, a DMZ, o uso de IDS híbrido é vantajoso uma vez que ataques específicos a cada servidor podem ser identificados com maior precisão.

5. Deficiências nos IDS

Uma deficiência da maioria dos sistemas de detecção de intrusão é o fato do seu funcionamento se basear no mesmo princípio dos sistemas antivírus, ou seja, utilizam bases de dados com assinaturas de ataques: se ataques conhecidos são detectados, as tentativas são bloqueadas com relativa facilidade, caso contrário, podem passar impunemente.

Outra questão potencialmente problemática tem a ver com o volume de dados gerado. Numa rede com elevados índices de atividade, os dados registados pelos sensores podem atingir proporções significativas, o que implica dificuldades na capacidade de detecção e de gestão. De fato, estes sistemas requerem acompanhamento em tempo real como forma de validação das ocorrências registadas. Se considerarmos ainda que, para além destes, existem registos dos servidores, routers, firewalls, antivírus, etc., a carga administrativa associada pode ser muito grande.

Nos casos em que se pretenda fazer uma gestão adequada da informação gerada pelos mecanismos de defesa, todos estes dados deverão ser cruzados, com vista à detecção de padrões e obtenção de informações sobre potenciais ataques.

Laureano (2002, p.3) destaca:

> A maior dificuldade relativo a um sistema de detecção de invasão [...] é identificar e classificar o que é realmente uma tentativa de acesso não autorizado ou simplesmente um erro eventual, ou uma distração para ocupar os administradores de sistemas enquanto o verdadeiro ataque ocorre.

A instalação de um IDS deve ser cuidadosamente avaliada. Regra geral, não são sistemas simples e seu custo cresce proporcionalmente com a capacidade de proteção desejada. Entretanto, todo o tempo dedicado ao planejamento de instalação de um IDS irá poupar tempo na gestão da informação gerada.

Os sensores de rede deverão ser instalados em máquinas dedicadas, nos pontos de entrada da infra-estrutura de comunicação e os sensores de host nos sistemas que se pretende proteger. Todos os sensores se comunicam com uma estação de gerenciamento central (ADM), onde são armazenados todos os dados coletados. Esta estação, que também deverá ser dedicada a esta tarefa, é o ponto da rede no qual se faz a gestão centralizada dos recursos IDS disponíveis (Fig. 2).

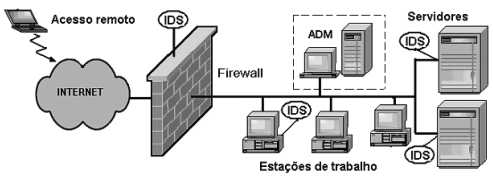

Figura 2 – Posicionamento da estação de gerenciamento central na rede

Idealmente, a infra-estrutura IDS deverá pertencer a uma rede dedicada, separada do restante da rede corporativa, não devendo os computadores com sensores de rede ser visíveis nesta última, ou seja, as suas placas de rede não devem possuir qualquer endereçamento, ou seja, devem operar em modo promíscuo.

As regras de monitoração devem ser afinadas de modo a responderem às reais necessidades da organização, ou seja, para os serviços que não sejam disponibilizados na rede, a existência de uma base de dados para a detecção de ataques poderá não se justificar. Deste modo consegue-se evitar a produção maciça de informação que não apresenta interesse real para a proteção da rede.

Ao lidar com estes dados, é necessário confirmar a sua aplicabilidade, ou seja, verificar se não se tratam de falsos positivos: um falso positivo é a identificação de uma atividade legítima como sendo um ataque. Os responsáveis pela segurança da rede deverão analisar os dados obtidos e confirmar se são ataques reais ou não.

Os dados relativos à atividade maliciosa registados pelo IDS podem ocasionar várias reações: alertas administrativos (incluindo chamadas para celulares) e reações automáticas (interrupção da conexão ou bloqueio do IP de origem, por exemplo).

6. Metodologias de Detecção

As metodologias utilizadas pelos IDS para a detecção de um ataque são o Knowledge-Based Intrusion Detection, ora conhecido como Misuse Detection System e o Behavior-Based Intrusion Detection, também conhecido como Anomaly Detection System.

6.1. Knowledge-Based Intrusion Detection

A abordagem Knowledge-Based Intrusion Detection, na qual as detecções são realizadas segundo uma base de dados com informações sobre ataques conhecidos, é a mais utilizada pelos IDS. O funcionamento, neste caso, é semelhante ao antivírus, pois o IDS procura por um padrão ou uma assinatura de ataque que esteja na sua base de dados.

Thomas (2007, p. 308) ratifica em sua obra:

> A equivalência de assinatura/padrão é o método mais comum de se detectar ataques, e significa que o IDS deve ser capaz de reconhecer cada técnica de ataque para ser efetivo. Um IDS possui grandes bancos de dados com milhares de assinaturas que permitem ao IDS encontrar padrões ou assinatura de ataques.

Todos os eventos que não são reconhecidos pelo conjunto de assinaturas são considerados aceitáveis. Consequentemente, a precisão desse tipo de IDS depende das atualizações da base de dados, do sistema operacional, da versão de IDS em uso, da plataforma e da aplicação.

6.2. Behavior-Based Intrusion Detection

O Behavior-Based Intrusion Detection considera que as tentativas de intrusão podem ser descobertas através de desvios no comportamento dos usuários ou dos sistemas. Um modelo de normalidade é estabelecido em condições adequadas de uso dos recursos (quando este não está sob ataque) e comparado com a atividade em andamento.

Qualquer comportamento suspeito dos pacotes que trafegam pela rede passa por uma análise estatística ou heurística com o objetivo de encontrar possíveis indícios de alterações de padrão, como súbito aumento de tráfego, utilização maciça da CPU, atividade anormal do disco rígido, entre outros. O que for diferente do padrão armazenado na base de dados será considerado suspeito.

7. Posicionamento dos Sensores

Um dos problemas para a utilização de IDS, especificamente do NIDS, é a segmentação cada vez maior das redes pela utilização de switches, o que faz com que o NIDS tenha limitações quanto ao seu desempenho, uma vez que ele funciona no modo promíscuo, analisando todos os pacotes que passam pelo segmento da rede.

É possível utilizar o NIDS em redes segmentadas por switches usando sensores HIDS em conjunto com o NIDS, nos IDS híbridos. Os sensores podem ser usados de diversas formas, as quais irão refletir o grau de monitoramento do ambiente de rede (Fig. 3):

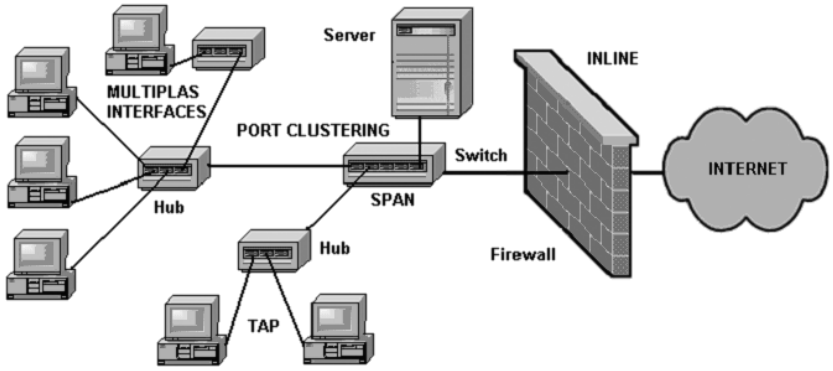

Figura 3 - Posicionamento dos sensores na rede

• **Switched Port Analyzer (SPAN) e hubs** – portas SPAN de switches ou portas de hubs pode ser usadas para que os sensores sejam habilitados;
• **Modo Tap –** os sensores são inseridos como uma extensão da rede (modo Tap);
• **Modo Inline –** O IDS é posicionado fisicamente no fluxo da informação, com o tráfego dos pacotes passando ativamente pelo sistema;
• **Port Clustering –** permite a monitoração dos segmentos da rede, com todos os tráfegos sendo agregados em um único fluxo de dados;
• **Múltiplas interfaces –** um sensor atuando em diferentes segmentos de rede.

7.1. Localização do IDS na Rede

O IDS pode ser utilizado em diversas posições na rede e cada posição significa um tipo de proteção específico. Outra consideração importante é quanto ao posicionamento do IDS em relação ao firewall da rede:

· Posicionado antes do firewall, a detecção é considerada simultânea aos ataques (detecção de ataques);
· Posicionado após o firewall, a detecção passa a ser de intrusões (detecção de intrusões) ou de erros cometidos pelos usuários internos (misuse).

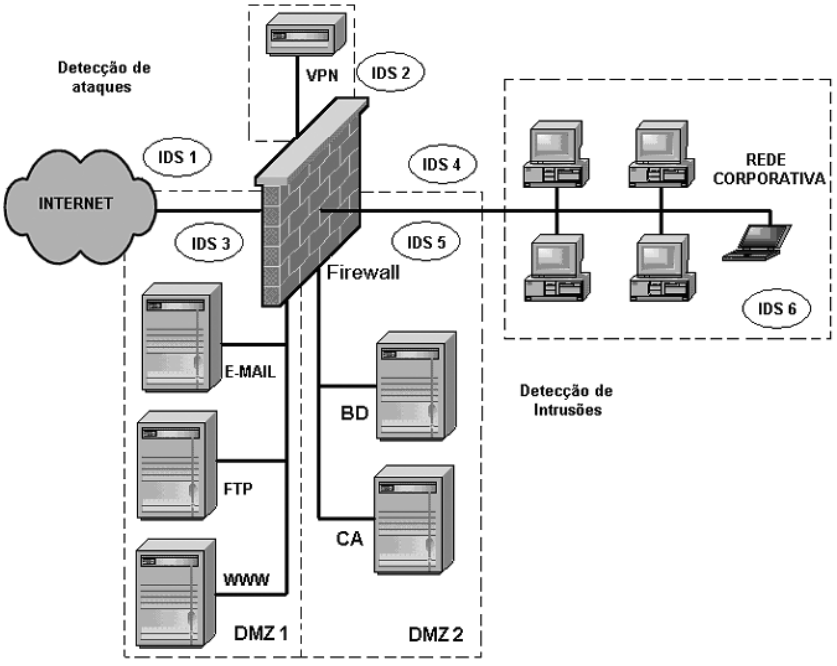

Figura 4 - Localização de IDS na rede

Na Fig. 4 temos os seguintes posicionamentos:

• **IDS 1 –** detecta tentativas de ataques externos, oferecendo uma fonte de informações sobre os tipos de ameaças de intrusão para a rede corporativa;
• **IDS 2 –** funciona no próprio firewall, detectando tentativas de ataque contra este;
• **IDS 3 –** detecta tentativas de ataque contra os servidores localizados na DMZ 1, que conseguem passar pelo firewall;

• **IDS 4 –** detecta tentativas de ataque contra recursos internos da rede que passaram pelo firewall e que podem ocorrer via VPN, por exemplo;
• **IDS 5 –** detecta tentativas de ataque contra os servidores localizados na DMZ 2, que passaram pelo firewall, pela VPN ou por algum outro serviço na DMZ 1;
• **IDS 6 –** detecta tentativas de ataques internos na rede corporativa.

8. Sistemas de Prevenção de Intrusões

O funcionamento do IDS como sniffer apresenta alguns problemas, como o fluxo de pacotes fragmentados, não confiáveis e que chegam fora de ordem. Os sistemas funcionam em modo passivo, apenas escutando o tráfego, não sendo capazes de controlar esse tráfego, seja ignorando, modificando, atrasando ou injetando pacotes para defender a rede.

A identificação desses pontos fracos, relacionados a determinados tipos de IDS, levou ao desenvolvimento de novos sistemas que buscam detectar e prevenir ataques contra a rede de comunicação. Operando de forma inline na prevenção de intrusões, eles são conhecidos como Sistemas de Prevenção de Intrusões (Intrusion Prevention System – IPS).

A operação inline difere da operação passiva na forma de capturar os pacotes dos segmentos de rede. Enquanto o IDS que opera no modo passivo captura o tráfego do segmento de rede, o IDS que opera no modo inline assume uma posição como um firewall, onde todo o tráfego da rede passa por ele (Fig. 5). Essa característica permite que o IDS inline seja capaz de detectar os ataques e também de preveni-los, pois os pacotes dos atacantes não chegam aos servidores da rede.

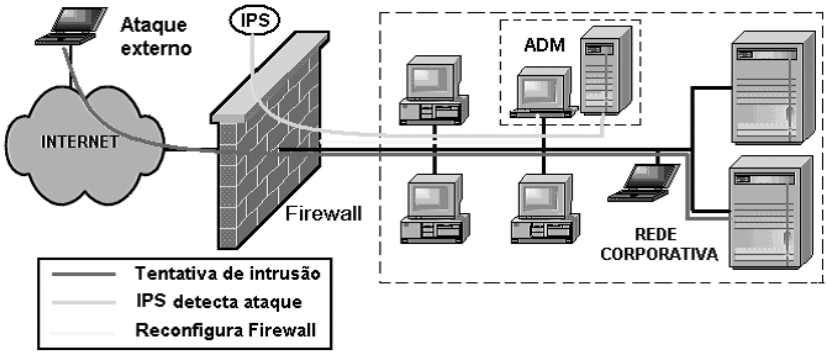

Figura 5 - Funcionamento do IPS na rede

A diferença entre os dois modos de operação (passivo e inline) torna-se clara: no modo passivo, o IDS é capaz de detectar ataques, mas não é capaz de preveni-los; no modo inline, o IDS é capaz de detectar ataques e evitá-los utilizando recursos semelhantes aos de um firewall.

9. Detecção de Anomalias

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.

9.1. Anomalias em Padrões de Comportamento

Os sistemas que procuram por anomalias em padrões de comportamento (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.

9.2. Anomalias em Padrões de Tráfego

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, pode-se considerar o gerenciamento de uma 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. 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.

9.3. Anomalias em Padrões de Protocolos

Os sistemas que procuram por anomalias em padrões 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.

É possível construir um modelo bastante rígido do que deve ocorrer e qualquer divergência com o modelo pode ser facilmente observada. Segundo Thompson (2004, p. 228) "O administrador poderá acessar o servidor da empresa de qualquer ponto de acesso a Internet e averiguar o grau de risco do ataque".

Outra vantagem desse sistema é que ele pode detectar uma grande variedade de anomalias dentro do espaço do protocolo, podendo ser construído com muita eficiência. A desvantagem, porém, é que pode ser difícil de estimar o efeito da anomalia observada de forma acurada, uma vez que alguns tipos de transações de protocolo problemáticas (como ataques, por exemplo) não se manifestam como anomalias.

10. Detecção de Vulnerabilidades

Este é um teste de simples execução, constando do confronto dos sistemas e aplicações existentes com listas de vulnerabilidades conhecidas. Atendendo ao enorme número de vulnerabilidades, estes testes são normalmente realizados com programas automáticos de detecção, contendo bases de dados de vulnerabilidades atuais (Fig. 6).

Recomenda-se a correção automatizada e/ou manual das vulnerabilidades detectadas, bem como um registo detalhado das ações realizadas.

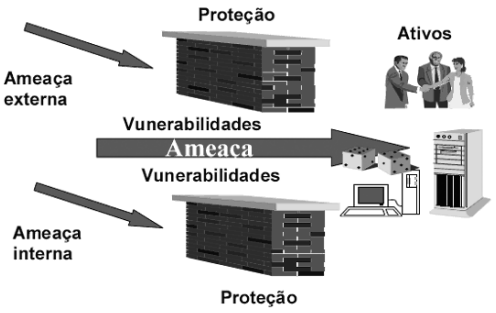

Figura 6 - Vulnerabilidades e ameaças nos sistemas de informação

10.1. Testes de Intrusão

Os testes de intrusão são tentativas de acesso aos sistemas da rede corporativa por parte de pessoas não autorizadas. Este tipo de análise poderá ser realizado sem qualquer conhecimento prévio dos sistemas a testar, ou com a indicação das respectivas características. Ambas as possibilidades têm pontos positivos e negativos: no caso da primeira, cria-se um cenário mais realista, na medida em que assumirá o ponto de vista de um hipotético atacante; no caso da segunda, em que existe o conhecimento completo das características dos sistemas a testar, garante-se a profundidade dos testes, pois estes irão provavelmente deixar menos vulnerabilidades de fora.

Estes testes podem ser realizados tanto a partir do interior da rede como a partir da Internet, dependendo a decisão sobre o ponto inicial do teste, das características da organização (número de sistemas, número de funcionários, tipo de aplicações) e dos resultados que possam ser obtidos da análise (Fig. 6). Em qualquer dos casos, convém, mais uma vez, garantir que os testes não sejam intrusivos e que os resultados sejam úteis e não apenas descrições de ataques.

10.2. Segurança Integrada

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

As tecnologias de segurança principais que podem ser integradas incluem:

- **Firewall -** Controla todo o tráfego de dados através da verificação das informações que entram e saem da rede a fim de garantir que não ocorram acessos não autorizados;
- **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 de pacotes não desejado na rede;
- **Redes Privadas Virtuais (VPN) -** Asseguram as conexões além do perímetro da rede local, permitindo que redes locais se comuniquem com segurança através da Internet;
- **Gerenciamento de Vulnerabilidade -** Permite a avaliação da posição de segurança da rede descobrindo falhas de segurança e sugerindo melhorias;
- **Proteção 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 de operação e manutenção são reduzidos.

11. Conclusão

A segurança, mais que simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, mais do que um supressor de sintomas, é um processo contínuo e abrangente, com implicações em todas as áreas, desde a alta direção até os usuários que executam operações cotidianas elementares, devendo ser encarada como um facilitador dos processos e como forma de aumentar os níveis de confiança internos e externos.

Tornar uma rede de computadores e os recursos relacionados menos vulneráveis às ameaças e aos ataques utilizando sistemas de detecção e prevenção de intrusões é uma atividade em permanente evolução, mutação e transformação, que requer um esforço constante para o seu sucesso e uma forte capacidade para provocar e gerir mudanças, tanto nos hábitos instituídos como na infra-estrutura de suporte da organização.

Há a necessidade de se desenvolver uma visão ampla desses sistemas que permitirá encarar de forma integrada a segurança da informação, considerando tanto o ponto de vista pessoal (quer seja técnico, de gestão ou outro), a especificidade dos sistemas envolvidos, bem como as necessidades do negócio da corporação.

12. Referências

· LAUREANO, Marcos Aurélio P. **Sistemas para Identificação de Invasão.** Curso de Informática Aplicada – PUC-PR. Curitiba, PR, 2002.

• MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar - ataques de hackers:** controlando o fator humano na segurança da informação. São Paulo: Pearson Education do Brasil Ltda, 2003.

• NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

• SILVA, P. T.; CARVALHO, H.; TORRES, C. B. **Segurança dos Sistemas de Informação**: Gestão Estratégica da Segurança Empresarial.

Lisboa: Centro Atlântico, 2003.

• STREBE, Matthew; PERKINS, Charles. **Firewalls 24Seven**, 2 ed. Alameda: Sybex, 2002.

• THOMAS, Tom. **Segurança de Redes** – Primeiros Passos. Rio de Janeiro: Ciência Moderna, 2007.

• THOMPSON, Marco Aurélio. **O Livro Proibido do Curso de Hacker**. Salvador: ABSI, 2004.

Informações bibliográficas:
Conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT), este texto científico publicado em periódico eletrônico deve ser citado da seguinte forma:
NOBRE, J. C. A.. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. Cadernos UniFOA , Volta Redonda, ano 2, nº. 5, dez. 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao/05/11.pdf>