VOLTAR

PROXY, VPN, VLAN, IPS, IDS, HONEYPOT, FIREWALL E DMZ.

Apresentar algumas das principais tecnologias utilizadas para a implementação da segurança lógica dentro das organizações que ajudarão a diminuir a possibilidade de acessos indevidos, bem como a utilização da rede por pessoas que não tem autorização para tal.

NESTE TÓPICO

Marcar tópico

Como vimos anteriormente, a segurança física buscará implementar controles para que um atacante ou pessoa mal-intencionados não tenham acesso aos equipamentos por onde os dados e as informações trafegam diariamente dentro das empresas. Porém, com o advento das redes locais e da internet, os computadores estão, além de fisicamente ligados, conectados por meio de uma rede de softwares que permitem que eles possam trocar informações entre si. Dessa forma faz-se necessária a implementação de alguns procedimentos técnicos para que a troca de dados entre os computadores, bem como a sua interação, possa ser feita de forma segura. Alguns controles como biometria e senhas já foram apresentados anteriormente, porém agora abordaremos algo mais específico.

Firewall

No passado, quando não existiam computadores e a invasão de uma empresa era feita de forma física, houve a necessidade de se criarem algumas barreiras de segurança que impedissem que o atacante entrasse na empresa. Um muro era construído de forma a separar o mundo exterior do mundo da empresa. Dessa forma, se alguém quisesse invadi-la, teria que primeiro passar por esse muro. É claro que se colocássemos um muro entre o mundo externo e o da empresa e não colocássemos uma porta, essa proteção acabaria impedindo que as pessoas que trabalhassem na empresa também não tivessem acesso ao ambiente. Por isso houve a necessidade de colocar uma porta no muro para que as pessoas autorizadas entrassem. Porém, devido à necessidade de várias pessoas entrarem nesse ambiente, criaram-se outras portas para facilitar o acesso e separar essa entrada de pessoas de acordo com a sua necessidade. O aumento da quantidade de portas por um lado facilita o acesso, porém aumenta a necessidade de controle, pois cada uma dessas portas significa um ponto de acesso que pode ser explorado por um possível invasor

Com base nesse cenário, podemos comparar o Firewall que funciona dentro de um ambiente de rede corporativo com o muro – sua função principal é a de ser o elemento que ficará na fronteira entre a rede interna e a externa da empresa. No mercado, o Firewall também é conhecido como "parede de fogo", pois será ele que isolará a empresa do mundo externo, atuando como uma barreira de segurança na fronteira da rede da empresa, controlando o acesso de seu site ou da rede interna. Também pode atuar como autenticador para acessos permitidos a sites, bem como consegue manter o registro de todo o tráfego que entra ou sai da rede. A implementação do Firewall pode ser feita por meio de hardware e por softwares.

Tipos de controles do Firewall

Existem diversos controles que um Firewall pode implementar, dentre eles podemos citar quatro tipos:

- **Serviço:** ao implementar esse tipo de controle, a ideia principal é determinar quais serão os serviços de rede que estarão disponíveis para acesso por parte dos usuários da empresa.
- **Sentido:** como o próprio nome diz, nesse tipo de controle o foco está relacionado à determinação da direção ou do sentido em que os serviços da rede podem ser iniciados.
- **Usuário:** nesse tipo de controle é aplicado o controle ao acesso que o usuário possui baseado no seu logon de rede, e com isso permite-se ou não o acesso a determinado serviço que o usuário esteja requerendo.
- **Comportamento**: controle em que é verificado como cada serviço de rede pode ser usado e qual o comportamento esperado por ele.

Para as máquinas-clientes do serviço de Firewall, tanto internas como externas, toda ação é totalmente transparente, e para elas é como se não existisse nenhum tipo de controle sendo executado. Só se percebe o controle quando se tem que autenticar ou alguma requisição feita por parte do usuário é proibida e lhe é retornada uma tela com mensagem de erro ou negação.

IDS

Muitas vezes agimos de forma reativa aos eventos que acontecem nas nossas vidas, seja por não estarmos preparados ou até mesmo por não acreditarmos que uma determinada situação possa ocorrer. Se estivéssemos preparados e vigilantes, talvez não conseguíssemos evitar o problema, mas estaríamos preparados para resolvê-lo. A ideia dessa introdução é exatamente fundamentar uma ferramenta de segurança que deve ser utilizada para identificar possíveis anomalias nos sistemas que possam ser indícios de uma tentativa de invasão.

A sigla IDS é uma abreviação para Sistema de Detecção de Intrusão. Um software de IDS busca identificar ações que estejam ocorrendo dentro de um ambiente de rede de computadores que possam significar um possível acesso ou operação feita de forma indevida.

Existem softwares de IDS que devem ser instalados dentro dos próprios servidores, bem como existem outros que são instalados dentro do segmento da rede onde esses mesmos servidores estão instalados logicamente. O primeiro tipo recebe o nome de HIDS – Host Intrusion Dectect Systens (Sistema de Detecção de Intruso para Equipamento), enquanto o segundo é conhecido como NIDS – Network Intrusion Destect Systens (Sistema de Detecção de Intruso para Redes).

Uma característica principal a ser destacada é que os HIDS apresentam poucos falsos positivos (capacidade da ferramenta de identificar algo como sendo um ataque, quando na realidade é uma atividade normal), ao contrário das ferramentas de NIDS, que apresentam um número elevado de falsos positivos uma vez que estão fazendo uma análise dentro do segmento da rede, e serviços e pacote de dados direcionados para os servidores podem ser vistos como possíveis ataques e fazer o alarme da ferramenta disparar.

Outra diferença é que o HIDS, por estar instalado na máquina a ser protegida, monitora atividade somente dessa máquina e com isso consegue ter melhor visibilidade do comportamento das aplicações individuais que estão rodando dentro dela. O NIDS é frequentemente colocado junto a um roteador ou Firewall com a função de analisar o tráfego, examinando cabeçalhos e conteúdo dos pacotes. Podemos citar como um problema a ser pensado com relação ao NIDS o fato de que todos os ataques têm origem pela rede, e, no caso de o ataque ocorrer diretamente na máquina, ele se tornará inútil.

Os IDS podem ser formados por hardware e software, que deverão trabalhar conjuntamente para tentar identificar algumas atividades inesperadas na rede ou nos equipamentos que podem ser um forte indicativo de que um ataque está acontecendo ou terá grande possibilidade de ocorrer. O tipo de IDS a ser utilizado dentro do projeto de segurança dependerá da necessidade de segurança a ser implementada, bem como dos custos e vulnerabilidades que se deseja atacar. A utilização de um IDS não protegerá 100% a rede da empresa, porém poderá diminuir o risco de uma invasão.

As ferramentas de detecção de intrusão também podem ser utilizadas com a intenção de auditar as configurações da rede em busca de vulnerabilidades, assim como analisar a integridade dos dados, entre outras coisas. Dependendo do método de detecção escolhido, existirão diversos benefícios diretos ou indiretos.

IPS – Intrusion Prevention System (Sistema de Prevenção a Intrusão)

O IPS, tem a capacidade de identificar uma intrusão, mas além disso, analisar a relevância de cada evento ocorrido e seu risco, e então bloqueá-los, aumentando assim a tradicional técnica de detecção de intrusos.

O IPS é uma ferramenta com inteligência na maneira de trabalhar, pois reúne componentes que fazem com que ele se torne um repositório de logs e técnicas avançadas de alertas e respostas, voltadas exclusivamente a tornar o ambiente computacional cada vez mais seguro sem perder o grau de disponibilidade que uma rede deve ter.

O IPS usa a capacidade de detecção do IDS junto com a capacidade de bloqueio de um firewall, notificando e bloqueando de forma eficaz qualquer tipo de ação suspeita ou indevida e é uma das ferramentas de segurança de maior abrangência, uma vez que seu poder de alertar e bloquear age em diversos pontos de uma arquitetura de rede.

Um IPS é instalado de forma que o equipamento consegue enxergar todo o tráfego em ambos os sentidos camada de registro para autenticação, comunicação e reportar condições de erro entre elas.

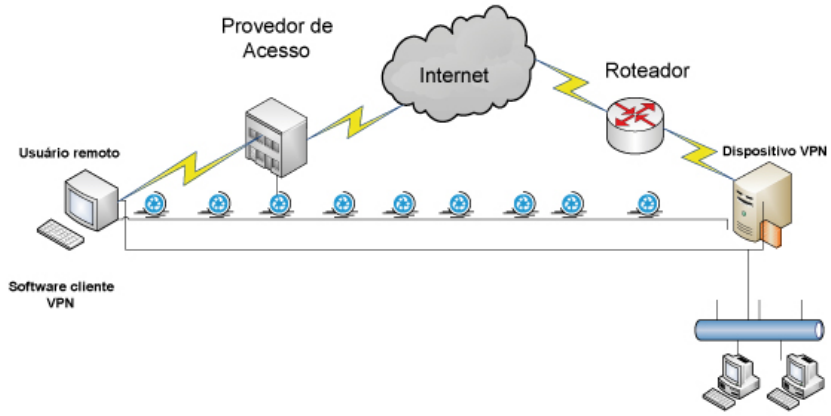
VPN

A sigla VPN vem da abreviação de Virtual Private Network (Rede Privada Virtual). A ideia da utilização da VPN como ferramenta de segurança está no fato de ela permitir que se faça uma conexão com a empresa de forma remota utilizando uma rede insegura como a internet.

Por meio de técnicas que permitem a criação de túneis virtuais criptografados , os computadores são conectados à empresa pela internet. A VPN permite também que as corporações se conectem entre si por meio da internet, construindo assim um Extranet. A VPN, além do foco da segurança, permite que a empresa tenha redução de custo com as comunicações corporativas, devido à não necessidade de utilização de links dedicados principalmente quando estamos nos referindo a conexões entre empresas de forma nacional ou internacional. Com esse cenário, as redes corporativas se estendem além de suas fronteiras físicas, possibilitando a conexão da empresa com suas filiais, parceiros e até mesmo à residência de seus colaboradores. A VPN possibilita a conexão dos computadores de qualquer lugar que tenha acesso à internet.

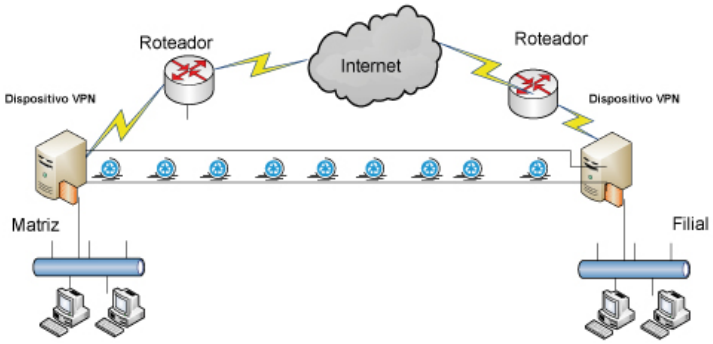
Os túneis presentes dentro da VPN podem ser criados de duas maneiras diferentes: túnel voluntário e túnel compulsório. No primeiro tipo a solicitação para a sua criação é feita através do software que está instalado na máquina do usuário até o servidor da empresa.

Na figura a seguir, podemos ver o exemplo de uma conexão de um usuário remoto à rede da empresa.



No túnel compulsório, como o próprio nome diz, ao contrário do que ocorre no túnel voluntário, para a criação da conexão com o ambiente da empresa não é necessário utilizar nenhum software que esteja instalado no equipamento do cliente para iniciar/criar o túnel virtual com a empresa.

Nesse processo, um equipamento da rede configura e cria um túnel de forma compulsória automaticamente para a máquina-cliente, e esta passa a acessar os recursos da rede remota através do túnel já existente, criado pelos equipamentos que estão nas extremidades das duas redes conectadas entre si. Na figura a seguir, podemos ver o exemplo de uma conexão entre a empresa e a sua filial.



VLAN

As *Virtual LANs* (VLANs) são redes virtuais que permitem segregar interfaces físicas de um switch gerenciável em mais de uma de LAN (*Local Area Network* – Rede Local), de maneira lógica, em diferentes grupos. Essencialmente, uma VLAN divide um switch físico, em um ou mais switches, com quantidade de portas igual ou menor que a quantidade total de portas do switch físico.

Aplicação

A separação das interfaces físicas de um switch (e, por consequência, dos dispositivos conectados a elas) em diferentes grupos beneficia:

- A segurança, uma vez que, naturalmente, as VLANs são isoladas umas das outras.
- A aplicação de regras específicas para uma determinada VLAN.
- A diminuição de custos, por diminuir a quantidade de switches físicos.
- O desempenho da rede, por criar mais domínios de *broadcast*.

Proxy

O Proxy pode ser entendido como um "procurador". Calma, não estou querendo dizer que é uma ferramenta de busca. Trata-se, na realidade, de uma ferramenta que possibilitará que uma máquina da rede haja em nome de outra. Como assim? O Proxy permite que os usuários internos de uma empresa acessem a internet por meio dele. Quando um usuário da rede interna digita um endereço da internet, que sai para o mundo externo em

busca da informação, é o endereço da máquina do Proxy; antes, porém, ele deve verificar se essa informação já foi solicitada anteriormente por outra pessoa e, caso já tenha sido, buscar no seu cache para repassar a informação ao solicitante. Se nenhum usuário tivesse solicitado a informação, o Proxy faria a pesquisa na internet e depois a repassaria para o usuário que a solicitou e, claro, armazenaria essa informação no seu cache.

A utilização do Proxy permite que a empresa centralize e gerencie a utilização da internet por parte dos funcionários, uma vez que todos os acessos para o mundo externo primeiramente têm de passar por ele. Com isso, algumas ações quanto à utilização da internet seriam facilmente implementadas, como: lista de sites que poderiam ser vistos, horário de utilização por parte dos colaboradores, lista de grupos de colaboradores que poderiam utilizar o serviço, aplicações que poderiam ser acessadas entre outras. Como tudo passa por ele, poderiam ainda ser implementados alguns procedimentos para logar as atividades dos usuários durante o acesso à internet e facilmente identificar as páginas que estão sendo acessadas e não estão relacionadas com as atividades profissionais do colaborador. Os Proxies também protegem as máquinas internas da rede de serem expostas diretamente à internet e são capazes de bloquear URL´s de site consideradas suspeitas ou perigosas.

Honeypot

Muitas vezes, para impedirmos um ataque, é necessário sabermos como ele será feito e quais armas serão utilizadas pelos atacantes, para que possamos responder corretamente com a medida de proteção adequada. No ambiente de rede, uma forma de se saber como um invasor de rede age e quais são suas ferramentas e técnicas de ataque é conseguida com a implementação de um equipamento que servirá como armadilha para ser explorado pelo atacante.

Esse conceito está relacionado à técnica de implementação, dentro de algumas redes, de um Honeypot, ou seja, "pote de mel". Um Honeypot geralmente é um sistema que é colocado em uma rede para que possa ser sondado e atacado; como não possui nenhum serviço específico rodando nele, não poderia ser acessado de forma alguma por usuários, tanto internos como externos. Caso ocorra uma interação com esse servidor, é um sinal de que alguém está tentando fazer algum acesso não autorizado ou está sendo feito algum tipo de sondagem no equipamento.

Tipos de Honeypot

Como exemplos de Honeypots, podemos citar dois tipos: Honeypot de produção e Honeypot de pesquisa:

- **Honeypot de produção**: é utilizado para distrair atividades maliciosas que um atacante possa lançar contra uma máquina da rede ou pode servir como um mecanismo de alerta para ajudar a ação dos IDS. A ideia também é tentar manter os invasores longe das máquinas verdadeiras e dos sistemas importantes, fazendo-os pensar que estão atacando os servidores verdadeiros.
- **Honeypot de pesquisa:** é utilizado para monitorar e estudar o comportamento dos atacantes. Consegue-se, com ele, a identificação dos códigos maliciosos que um invasor possa querer utilizar contra a sua rede, identificar possíveis varreduras e ataques, além de, com base nos ataques praticados pelo atacante, identificar as possíveis vulnerabilidades e com isso poder implementar medidas de proteção/ correção. Também consegue-se com isso descobrir os interesses e quais os alvos reais de um possível atacante o seu site.

DMZ – Zona Aberta (DMZ – Desmilitarized Zone)

Dentro da segurança técnica, as DMZ são segmentos de uma rede da empresa que devem estar acessíveis para usuários que fazem conexões por outras redes externas como, por exemplo, a internet. A DMZ tem como objetivo principal sediar equipamentos que recebam conexões vindas de fora da rede da empresa, e por isso esse segmento de rede deve conter servidores que não armazenem dados ou informações críticas ou importantes serviços da rede. Em um dos braços da DMZ está a *zona interna,* que é um seguimento de rede desenhado para guardar informações importantes, como bases de dados, senhas, cadastros, arquivos privados, sistemas de informação críticos para a empresa e que não devem receber conexões vindas do mundo externo; dessa forma, essas zonas deverão estar configuradas de maneira que somente usuários autorizados possam acessar diretamente seus equipamentos.

Quiz

Exercício Final

PROXY, VPN, VLAN, IPS, IDS, HONEYPOT, FIREWALL E DMZ.

Marcar este tópico como lido

INICIAR

Referências

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. *Segurança de redes em ambientes cooperativos*. São Paulo: Berkeley, 2002.

NORTHCUTT, Stephen; NOVAK, Judy; MCLACHLAN, Donald. *Segurança e prevenção em redes.* São Paulo: Berkeley, 2001.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003.

STREBE, Matthew; PERKINS, Charles. *Firewalls*, São Paulo: Makron Books, 2002.

Avalie este tópico

ANTERIOR
Tipos de vírus de computador: Worm, Trojan, Hoax, Backdoor e outros.

Índice

PRÓXIMO
Introdução à criptografia

uninove/biblioteca/sobre-a-biblioteca/apresentacao/)
Portal Uninove (http://www.uninove.br)
Mapa do Site