Segurança

Segurança é um ponto super importante a ser observado nas redes de computadores e precisamos prestar muita atenção para não deixar nenhuma vulnerabilidade exposta. É muito comum vermos nos jornais ou redes sociais que tal empresa sofreu um ataque, teve os seus dados sequestrados ou então teve uma indisponibilidade no sistema devido a um ataque de negação de serviço, também conhecido como **DoS**.

Quando falamos de segurança, devemos destacar dois tipos: física e lógica.

Podemos associar a segurança física à proteção dos nossos dados, como por exemplo deixar os servidores e equipamentos de redes em locais isolados, seguindo as normas do cabeamento estruturado. Geralmente em grandes empresas esses equipamentos ficam em salas separadas, com alta segurança e com a entrada permitida de poucas pessoas.

* **Proteção física**

É muito importante aplicar uma proteção física do ambiente, garantir que está protegido do acesso de pessoas não autorizadas, que possui sistemas de controle de temperatura, contingências para falhas de energia e até mesmo para suprir a falta de algum provedor externo, como por exemplo uma redundância que garanta que caso um provedor de internet ISP esteja em falha, outro provedor já seja estabelecido como o principal.

O controle de acesso é extremamente importante, seguir o princípio do least privilege indica que os colaboradores só devem ter o mínimo acesso possível para executar determinada função, dessa forma garantimos que pessoas indevidas não tenham mais acessos do que deveriam.

O caso muito comum e conhecido é a engenharia social. Nele o atacante procura levantar o máximo de informações sobre o alvo, no nosso exemplo a empresa procura brechas para acessar os sistemas. Entre as táticas de ataque pode-se ter uma aproximação com determinado funcionário a fim de conhecer mais sobre a vida dele e então realizar uma coerção que obrigue o funcionário a passar alguma informação sigilosa da empresa ou então comprometer o ambiente através de um pendrive infectado, por exemplo.

* **Proteção lógica:**

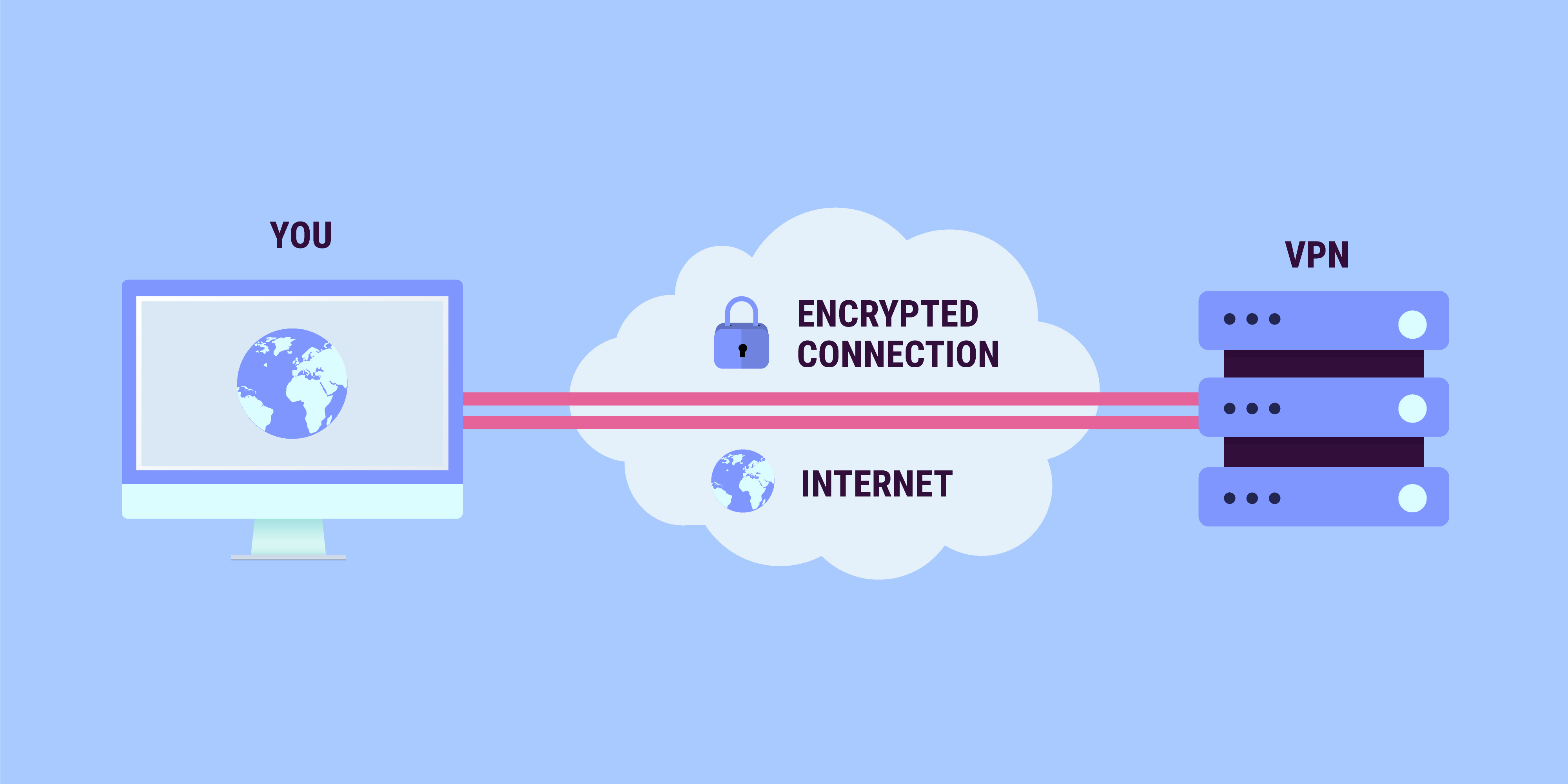
Essa é tão importante quanto a física. Nela podemos destacar cuidados ao nível lógico e de software da nossa rede.

Podemos destacar cuidados como sempre trocar a senha dos roteadores, switches e servidores. Nunca deixar senhas padrões. Usar um cofre de senhas para armazenamento seguro, assim sem a necessidade de ficar memorizando todas as senhas ou pior anotando em bloco de notas, configurar o SSO (Single Sign On) para permitir que os usuários usem a mesma senha de acesso a rede no acesso aos demais serviços, por exemplo o colaborador poderia usar a mesma senha que usa para entrar no computador, poderia entrar no sistema de RH, faturamento etc.

Outro serviço super importante que devemos ter na nossa rede é o Firewall, ele é um software responsável pela proteção da rede, podemos dizer que ele é o nosso guardião. Tem a função de identificar quais requisições estão chegando na rede, de onde vem, qual é o destino, qual porta será acessada e o que será enviado. Ele pode escanear essa requisição e caso julgue perigoso recusá-la.

# VPN

Todos nós sabemos que a internet é muito boa mas ao mesmo tempo super perigosa. Uma forma de trafegar os dados sensíveis na internet é com a utilização de VPNs (Virtual Private Network). Ela tem a função de criptografar os dados que são trafegados na internet. Podemos dizer que uma empresa tem a sua sede em São Paulo e uma filial no Rio de Janeiro e elas precisam se comunicar pela internet de forma segura , então é criado um túnel lógico entre os roteadores das duas empresas e estabelecida uma conexão criptografada que irá ocorrer sobre um protocolo de VPN como o OpenVPN ou IPsec.



* **Site to Site**

Conexão Empresa para Empresa, exemplo matriz e filial.

* **Cliente to Site**

Conexão Empresa para Cliente, exemplo funcionário em home office que realiza acesso a rede da empresa de uma rede do próprio cliente.

# Principais Ataques

* **Ransomware**

Por fim, outro ponto super importante: precisamos configurar o sistema de backup. Realizar cópia dos arquivos de configurações dos nossos dispositivos de redes, dos dados dos servidores e de toda informação da nossa empresa é crucial, pois em algum caso de falha a operação pode ser restabelecida se houver um sistema de backup. Um ataque que está em alta é o Ransomware, nele o atacante consegue penetrar na rede do alvo e criptografa todos os dados dos servidores impedindo a operação da empresa. Para descriptografar esses dados, o atacante solicita uma quantia em dinheiro que deve ser paga em uma conta fantasma em bitcoin. No caso da empresa atacada, caso não tenha backup dos arquivos pode perder todos os seus dados ou correr o risco de pagar o resgate dos arquivos com a ameaça de não tê-los de volta, além de sofrer com a grande exposição negativa desse ataque e correr o risco de acabar com a existência da empresa.

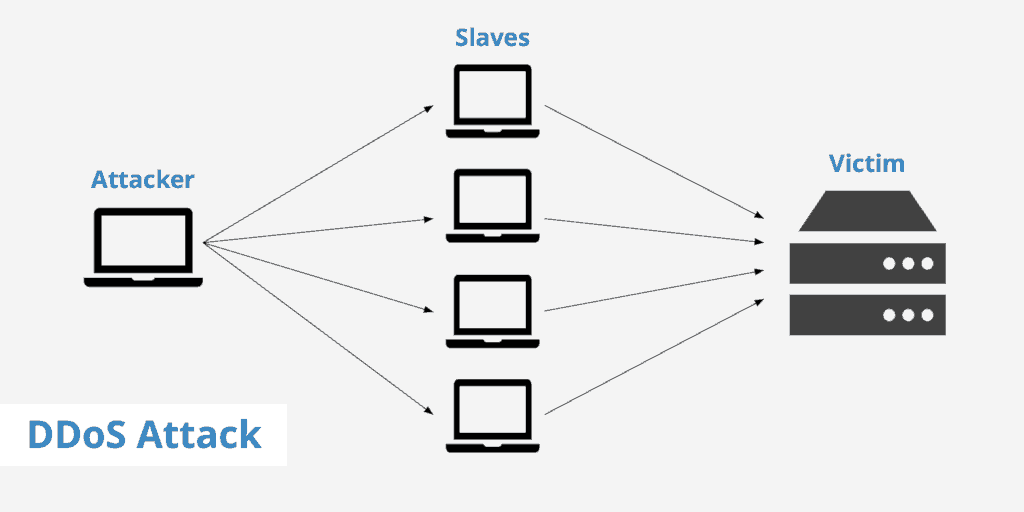


* **DoS (Denial of Service)**

Ataque de negação de serviço. O atacante infecta uma máquina que começa a enviar várias requisições em direção ao alvo do ataque. A ideia é causar a indisponibilidade do serviço que está sendo atacado.

* **DDoS (Distributed Denial of Service)**

Segue a mesma linha do ataque DoS porém ao invés do ataque vir de uma única origem ele vem de vários pontos, assim fica mais difícil de se proteger. O atacante replica um vírus em massa transformando várias máquinas em "zumbis" que começam a enviar requisições ao alvo.



* **SQL Injection**

Este ataque busca encontrar as vulnerabilidades expostas pelos sistemas e aplicações. O objetivo do SQL Injection é executar instruções SQL através de brechas da aplicação e assim obter dados do banco de dados em produção. Com este tipo de ataque é possível colher informações sobre os clientes e suas respectivas movimentações.

* **Main in the middle MITM**

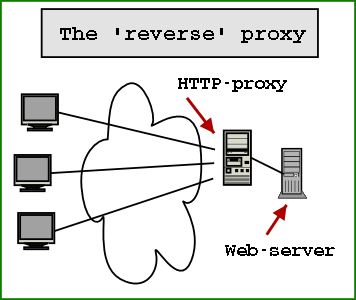
É um ataque caracterizado no qual o atacante fica entre o alvo e o sistema que ele está acessando. A ideia é ficar monitorando o que o atacado está fazendo e receber as informações dos seus acessos. Imagine que o usuário está acessando uma transação bancária, o atacante ficaria no meio da conexão entre o usuário e o banco, assim ele iria colher informações importantes sobre o alvo e realizar os ataques com precisão.

# Proxy

É o serviço responsável pela filtragem. O Proxy tem o intuito de trabalhar em conjunto com o firewall da rede e ele irá filtrar as requisições que estão saindo da rede. O Proxy ficará entre o computador requisitante e o servidor de destino, mantendo assim a privacidade da origem. Podemos pensar no cenário em que os desenvolvedores estão criando uma aplicação e precisam de dependências externas, estas estão localizadas em repositórios de terceiros e podem conter arquivos perigosos e vírus maliciosos, a ideia do Proxy é garantir que ao tentar baixar os arquivos desses repositórios os desenvolvedores recebam um erro e só consigam baixar os arquivos do repositório homologado pela própria empresa que pode garantir que os arquivos que estão ali são seguros.

* **Proxy reverso**

A utilização do Proxy reverso é uma boa forma de filtrar informações que estão chegando da Web em direção ao servidor. Podemos pensar no exemplo em que a empresa oferece uma aplicação Web através de um servidor como o Nginx e então é configurado um Proxy reverso para filtrar as requisições que estão chegando dos clientes em direção ao servidor, garantindo veracidade delas.



# Pentests

É o profissional capaz de realizar testes de segurança em determinada empresa. O objetivo do pentest é explorar todas as vulnerabilidades possíveis da rede e dos sistemas da empresa, após realizar esse levantamento é informado aos donos da empresa quais são as brechas de segurança e alinhando com o departamento de T.I. formas de correção e melhorias futuras. Existe tanto o pentest ético que analisa brechas com o intuito de melhorar brechas de segurança como também o criminoso que busca oportunidades de lucrar com essas falhas.