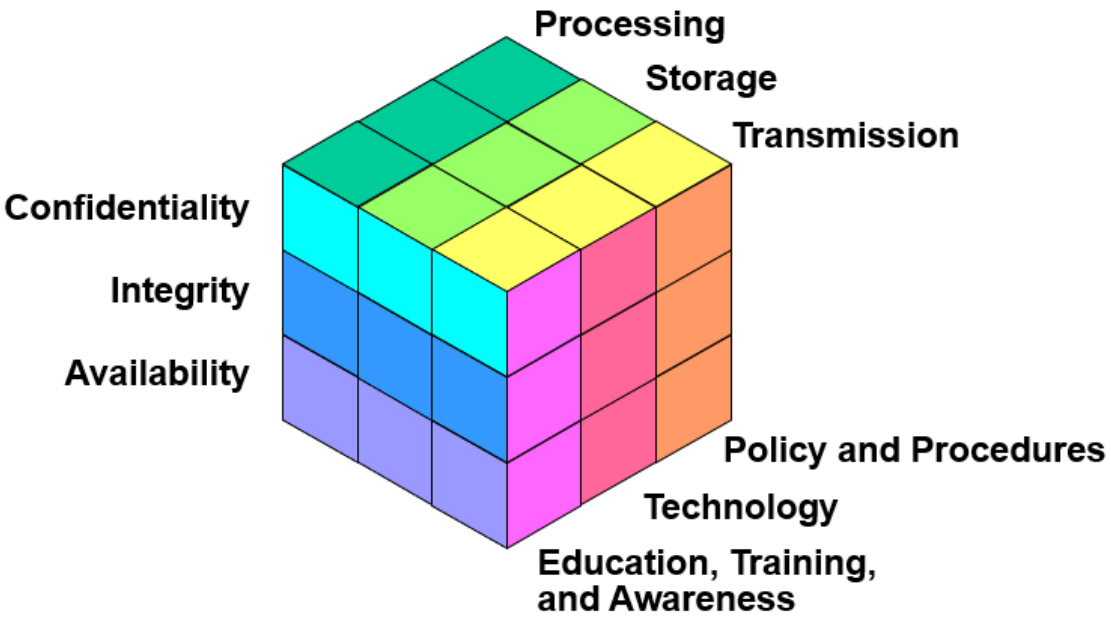
- **3 faces do cubo**



- **3 pilhares de segurança de informação**

Confidencialidade

Integrity

Disponibilidade

- **o que sao ameaças, vunerabiliadde, risco**

- quais os tipos de familias de ataques

Reconhecimento

Acesso

Negação de serviços

Worms, vírus e cavalos-de-Troia

Reconhecimento:

Initial query of a target

Ping sweep of the target network

Port scan of active IP addresses

Vulnerability scanners

Exploitation tools

Acesso:

A few reasons why hackers use access attacks:

To retrieve data

To gain access

To escalate access privileges

A few types of access attacks include:

Password

Trust exploitation

Port redirection

Man-in-the-middle

Buffer overflow

IP, MAC, DHCP spoofing

Denial of Service:

Hacker builds a network of infected machines

A network of infected hosts is called a botnet.

The compromised computers are called zombies.

Zombies are controlled by handler systems.

Zombie computers continue to scan and infect more targets

Hacker instructs handler system to make the botnet of zombies carry out the DDoS attack

- o que consiste uma politica de segurança

A document that states how an organization plans to protect its tangible and intangible information assets

Management instructions indicating a course of action, a guiding principle, or appropriate procedure

High-level statements that provide guidance to workers who must make present and future decisions

Generalized requirements that must be written down and communicated to others

- o que é um modelo AAA baseado

Authentication / Authorization / Accounting

As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

- firewalls

All firewalls:

Are resistant to attack

Are the only transit point between networks because all traffic flows through the firewall

Enforce the access control policy

- tipos de firewalls

Packet Filtering Firewall

Application Gateway Firewall

Stateful Firewall

NAT Firewall

- falar das gerações

Primeira Geração - Filtros de Pacotes

Restringir tráfego baseado no endereço IP de origem ou destino;

Restringir tráfego através da porta (TCP ou UDP) do serviço.

Segunda Geração - Filtros de Estado de Sessão

Todas as regras da 1ª Geração;

Restringir o tráfego para início de conexões (NEW);

Restringir o tráfego de pacotes que tenham sido iniciados a partir da rede protegida (ESTABLISHED);

Restringir o tráfego de pacotes que não tenham número de sequência corretos.

Firewall Statefull: Armazena o estado das conexões e filtra com base nesse estado. Existe três estados para uma conexão:

NEW: Novas conexões;

ESTABLISHED: Conexões já estabelecidas, e;

RELATED: Conexões relacionadas a outras existentes.

Terceira Geração - Gateway de Aplicação

Todas as regras das gerações anteriores;

Restringir acesso FTP a usuários anônimos;

Restringir acesso HTTP para portais de entretenimento;

Restringir acesso a protocolos desconhecidos na porta 443 (HTTPS).

Quarta Geração e subsequentes

O firewall consolida-se como uma solução comercial para redes de comunicação TCP/IP;

Stateful Inspection para inspecionar pacotes e tráfego de dados baseado nas características de cada aplicação, nas informações associadas a todas as camadas do modelo OSI (e não apenas na camada de rede ou de aplicação) e no estado das conexões e sessões ativas;

Prevenção de Intrusão para fins de identificar o abuso do protocolo TCP/IP mesmo em conexões aparentemente legítimas;

Deep Packet Inspection associando as funcionalidades do Stateful Inspection com as técnicas dos dispositivos IPS;

A partir do início dos anos 2000, a tecnologia de Firewall foi aperfeiçoada para ser aplicada também em estações de trabalho e computadores domésticos (o chamado "Firewall Pessoal"), além do surgimento de soluções de firewall dedicado a servidores e aplicações específicas (como servidores Web e banco de dados), ou mesmo usuários.

ACLs

ACL é uma lista sequencial de instruções de permissão ou negação que se aplicam a endereços ou protocolos forma eficiente de controlar o tráfego dentro e fora da rede; fornece segurança. A filtragem de pacotes controla o acesso à rede; Um router com ACLs configuradas funciona como um filtro, ao encaminhar ou negar de acordo com as regras estabelecidas; A filtragem ocorre na camada de Internet do TCP (L3)

ACLs padrão

As ACLs padrão permitem a você permitir ou negar tráfego de endereços IP de origem. O destino do pacote e as portas envolvidas não importam.

ACLs estendidas

As ACLs estendidas filtram pacotes IP com base em vários atributos, por exemplo, tipo de protocolo, endereço IP de origem, endereço IP de destino, portas TCP e UDP de origem, portas TCP e UDP de destino e informações do tipo de protocolo opcionais para maior granularidade de controle. Na figura, a ACL 103 permite tráfego com origem em qualquer endereço na rede 192.168.30.0/24 para qualquer host de destino na porta 80 (HTTP). As ACLs estendidas são criadas no modo de configuração global.

Podem tornar-se:

ACLs dinâmicas

ACLs reflexivas

ACLs baseadas em tempo

IPS/IDS

Ambas são "sensores"

Usam assinaturas para detetar padrões

Podem detetar padrões atómicos ou compostos (single-packet e multi-packet, respetivamente)

IDS

funciona passivamente

o tráfego tem de ser colocado noutra porta para chegar à IDS

vantagens:

não tem grande impacto de desempenho na rede

desvantagens:

mais vulnerável a técnicas de evasão

é preciso uma afinação correta para respostas

IPS

monitoriza tráfego L3 e L4

evita que ataques de pacote único cheguem ao destino

responde imediatamente

vantagens:

analiza todos os pacotes

desvantagens:

maior impacto de desempenho na rede

-tipos de criptografia

Simétrica

A criptografia simétrica é a técnica mais antiga e mais conhecida. Uma chave secreta, que pode ser um número, uma palavra ou apenas uma sequência de letras aleatórias, é aplicada ao texto de uma mensagem para alterar o conteúdo de uma determinada maneira. Isso pode ser tão simples quanto deslocar cada letra do alfabeto em diversos locais. Desde que o remetente e o destinatário saibam a chave secreta, eles podem criptografar e descriptografar todas as mensagens que usam essa chave.

DES, 3DES, AES, IDEA

Assimétrica

O problema com chaves secretas está em trocá-las pela Internet ou por uma grande rede e ao mesmo tempo impedir que caia em mãos erradas. Qualquer pessoa que conheça a chave secreta pode descriptografar a mensagem. Uma solução é a criptografia assimétrica, em que há duas chaves relacionadas - um par de chaves. Uma chave pública é disponibilizada gratuitamente a qualquer pessoa que queira enviar uma mensagem. Uma segunda chave privada é mantida em segredo, para que somente você saiba.

diffen-hellman (DH5+)

O método da troca de chaves de Diffie-Hellman permite que duas partes que não possuem conhecimento a priori de cada uma, compartilhem uma chave secreta sob um canal de comunicação inseguro. Tal chave pode ser usada para encriptar mensagens posteriores usando um esquema de cifra de chave simétrica.

- o que é boa pratica em termos de segurança à rede

implementar autenticação, desativar predefenições, etc

- indicar 5 praticas de programação segura

incriptação de dados, verificar input do user

VPN

Remote-Access VPN

Site-to-Site VPN Access

It's **Virtual**...because it's as if you have a private connection directly to any website or another computer you connect to.
It's **Private**...because all your website visits and online activity is between you and the websites you visit.
It's a **Network**...because you're using a special network of VPN servers that covers the entire globe.