

que é Segurança Cibernética

G3- SCCP

conceito:

Segurança cibernética é a forma de proteger seus sistemas como exemplo computadores e redes de possíveis ameaças digitais. Esses ataques buscam invadir, alterar e danificar os dados confidenciais de determinado usuário.



Importância



A segurança cibernética é muito importante porque são implementadas com o objetivo de minimizar os danos de uma invasão ou outras ações maliciosas, assim com a empresa utilizando este método consegue não afetar sua reputação e o cliente vai manter a confiança na empresa



História



Embora em 1950 surgia os computadores e modens, foi só em 1967 que começaram a se preocupar com esse tema porque a empresa IBM (International Business Machine Corporation) chamou diversos estudantes para testarem os computadores da empresa e perceberam que esses estudantes estavam cada vez mais aprofundados nessa tecnologia, com isso conseguindo acessar dados privados da empresa.

Mas este não havia sido o verdadeiro nascimento da segurança cibernética, pois só ocorreu em meados de 1970 com a ARPA desenvolvendo junto com a Força Aérea dos Estados Unidos protocolos de segurança para o sistema operacional Honeywell Multics. Porém foi na década de 1980 com o conflito tenso entre os EUA e a URSS(União das Repúlicas Socialistas Soviéticas) que foi a causa de um aprimoramento na segurança cibernética visando combater a espionagem digital.



Como Funciona?

Para realizar protocolos de segurança cibernética as organizações contratam especialistas em segurança digital com intuito de criar estratégias para proteger os dados. Os especialistas avaliam os possíveis riscos nos sistemas como redes, computadores, aplicações e outros dispositivos. Assim, quando avaliados eles criam uma estrutura de segurança que acrescente medidas contra os possíveis riscos de invasões na organização, tornando-a cada vez mais completa e livre de problemas.

Tipos de Cibersegurança



Uma estrutura de segurança cibernética contém camadas de proteção para se proteger de crimes cibernéticos, por isso se criam contramedidas para estas invasões, como:

Segurança de Infraestrutura Crítica: Ela protege os sistemas de computadores, aplicativos, redes e outros dos quais são importantes para a sociedade para uma segurança nacional, saúde econômica e segurança pública.

● **Segurança de Rede:** Tem foco em impedir o acesso não autorizado aos dados na rede, interrompendo ataques e violações. E também garantindo aos usuários autorizados um acesso seguro aos dados.

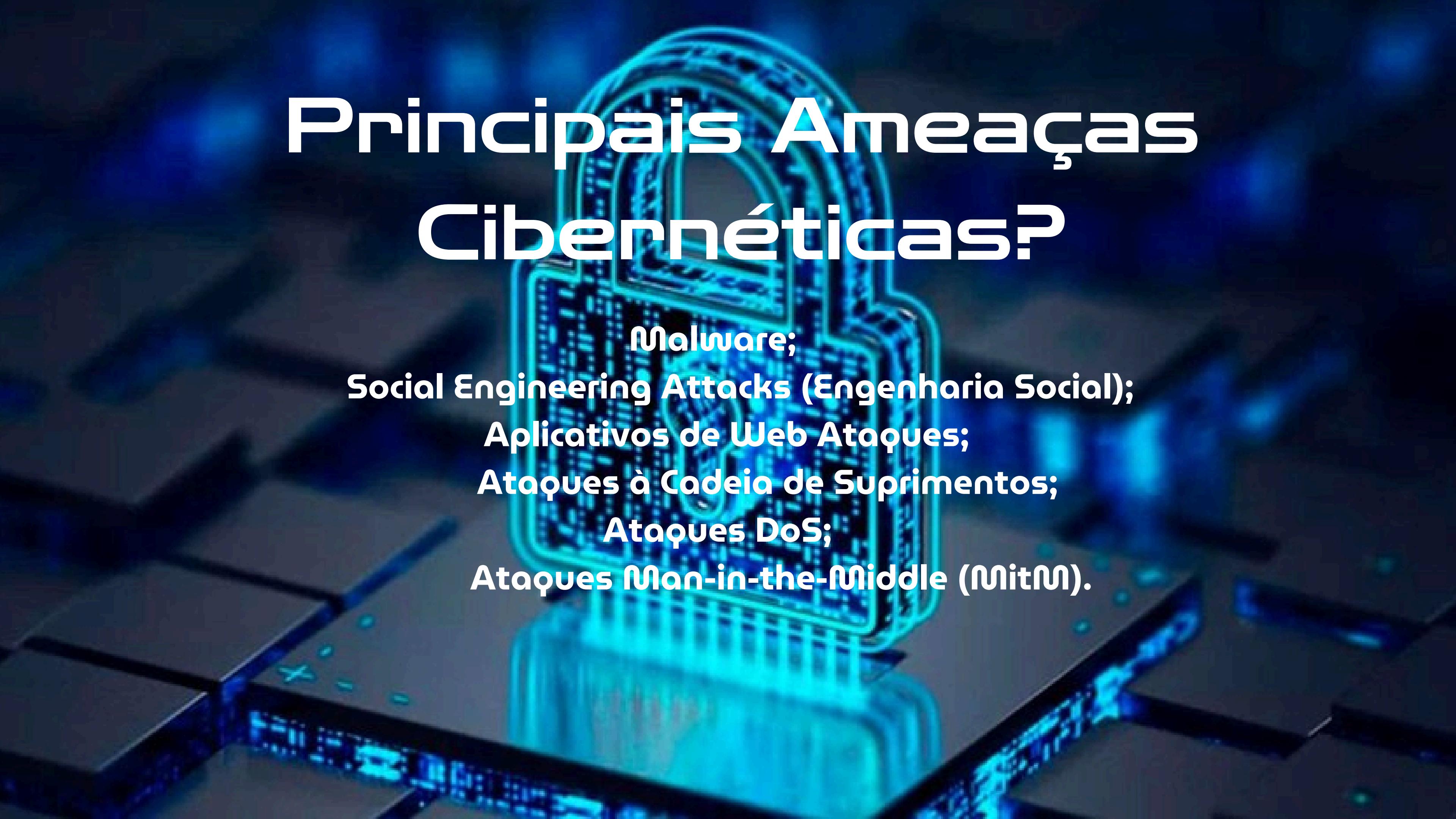
● **Segurança de Endpoints:** Os endpoints(servidores, desktops, laptops e dispositivos móveis) é o principal alvo de ataques digitais. Ela protege seus dispositivos e usuários que utilizam os endpoints para invadir.

Tipos de Cibersegurança



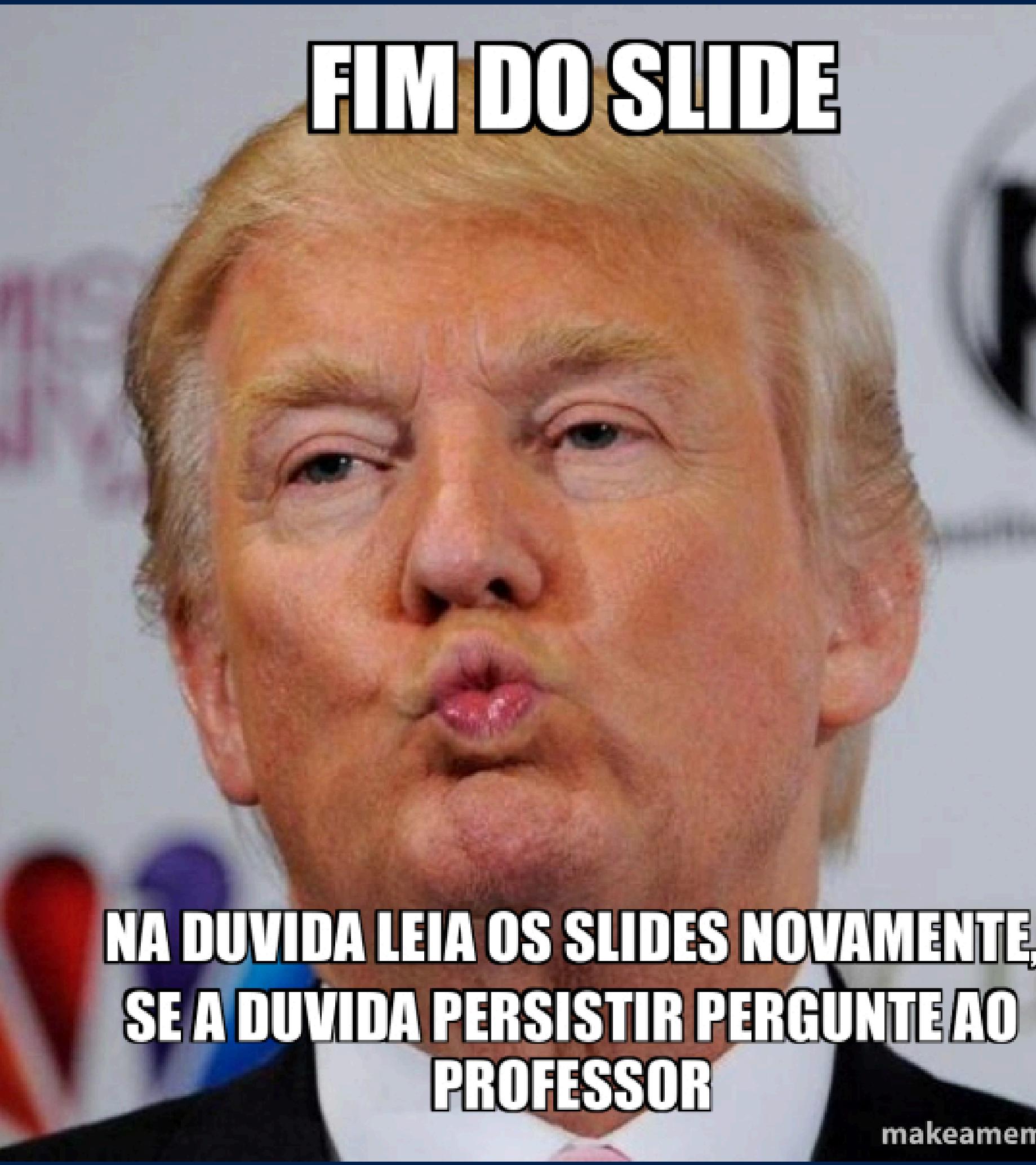
- **Segurança de Aplicativos:** Sua finalidade é proteger os aplicativos executados no local e na nuvem, impedindo o acesso não permitido aos aplicativos e dados relacionados, e evitando problemas na estrutura do aplicativo para os hackers não acessarem a rede.
- **Segurança na Nuvem:** Protege os serviços e recursos relacionados na nuvem, como aplicativos, dados, armazenamento e outros. A segurança é feita de modo compartilhada, o provedor da nuvem tem responsabilidade em proteger os serviços e infraestrutura usada, enquanto o cliente precisa manter confidencial os seus dados, código e outros recursos.
- **Segurança da Informação:** Refere-se à proteção dos principais dados da organização, sendo arquivos, dados digitais, mídia física, e outros documentos contra acesso as invasões.
- **Segurança Móvel:** A segurança móvel tem uma série de tecnologias para dispositivos móveis, com gerenciamento de aplicativos móveis (MAM) e o gerenciamento de mobilidade empresarial (EMM). E, atualmente ela serve para solucionar um problema no gerenciamento unificado de endpoints (UEM) melhorando a segurança na configuração dos endpoints.

Principais Ameaças Cibernéticas?



Malware;
Social Engineering Attacks (Engenharia Social);
Aplicativos de Web Ataques;
Ataques à Cadeia de Suprimentos;
Ataques DoS;
Ataques Man-in-the-Middle (MitM).

FIM DO SLIDE



**NA DUVIDA LEIA OS SLIDES NOVAMENTE,
SE A DUVIDA PERSISTIR PERGUNTE AO
PROFESSOR**

makeamem