SISTEMAS COMPUTACIONAIS E SEGURANÇA

Prof. Robson Calvetti

Alunos

Eduardo de Oliveira
Gustavo Andrade
Ian Bastos
Matheus Fraga

•Cibersegurança

Área da segurança da informação que visa a proteger dados contidos em dispositivos como servidores, computadores, redes e aplicações contra vazamentos, ataques e invasões. Essa prática envolve a segurança de dados, a recuperação de desastres e a continuidade do negócio. Inserir um pouquinho de texto

•Ciberataque

Um ciberataque é uma ação realizada por hackers ou grupos maliciosos com o objetivo de comprometer a segurança de sistemas computacionais, redes ou dispositivos.

Tipos de ciberataque:

-Ataques de engenharia social: manipulação de pessoas para obter informações

-Invasões de rede: acesso não autorizado a redes para roubar informações ou causar danos

-Exploração de vulnerabilidade: aproveitamento de falhas em softwares ou sistemas para infiltrar-se e realizar ações maliciosas

-Exfiltração de dados: roubo de informações sensíveis, como dados financeiros ou pessoais do usuário

•Segurança de redes

Na área relacionada às redes, os atacantes tendem a explorar tanto o tráfego de dados quanto os dispositivos físicos, que podem ter sido mal configurados. Realizando ataques como Information Gathering (o atacante obtém informações da rede – como, por exemplo, blocos de IP, certificados SSL, entre outras – para explorar possíveis vulnerabilidades), Session Hijacking (mascara tanto o cliente como o servidor, para que ambos acreditem estar se comunicando legitimamente).

O uso de firewalls e de criptografia podem ajudar a bloquear o acesso indesejado

- **Firewall**

Firewalls podem ser vistos como barreiras ou gateways que gerenciam o percurso de atividades da Web permitidas e proibidas em uma rede privada. O termo vem do conceito de paredes físicas como barreiras para retardar a propagação do fogo até que os serviços de emergência possam extingui-lo. Em comparação, os firewalls de segurança de rede são usados para gerenciamento de tráfego da Web. Normalmente, são destinados a retardar a propagação de ameaças da Web.

•Análise de vulnerabilidade

O objetivo dessa análise é garantir que a segurança de sistemas tecnológicos estejam em dia para garantir que eles não estejam sujeitos a ataques cibernéticos. Essa análise avalia a conformidade do sistema com as normas de segurança, procura pontos fracos, falhas de segurança e etc.

- **análise feita através de um mapeamento dos sistemas, aplicações e redes**
- **verificação das normas padrão de segurança**

•Criptografia

A Criptografia é uma técnica utilizada para codificar dados e informações digitais, para que terceiros não consigam acessá-las. Com o uso desse método as informações se tornam quase impossíveis de serem decifradas por aqueles que não tem a autorização de acessar as mesmas. De maneira geral, o processo permite converter dados legíveis em um formato codificado para torná-los inacessíveis. Para isso, normalmente os sistemas criptográficos usam um texto cifrado (ciphertext) baseado em chave para encobrir o texto simples (plaintext).