Ambientes Computacionais e Conectividade

Caio Henrique, Julia Helena, Giovanna Ribeiro Vasconcellos, Giovana Ayumi, Thalita Reis, João Victor de Souza Costa

Criptografia

A criptografia é fundamental para garantir a segurança dos dados pessoais e proteger as informações sensíveis contra acessos não autorizados. Ela armazena dados e comunicação entre dispositivos.

Tem como objetivo proteger os dados ao armazenas arquivos etc.

exemplo: icloud (Apple)

Firewall

O *firewall* é uma camada de segurança que monitora e controla o tráfego de dados entre redes, protegendo seu sistema contra acessos não autorizados. Seu objetivo é proteger o sistema ao bloquear acessos indesejados e permitir o fluxo seguro de informações autorizadas. A função do firewall se assemelha a uma “porta de segurança” que controla o que entra e sai da rede, ajudando a prevenir ataques de hackers, malware e tentativas de invasão.

Exemplo: *Firewall de Hardware*

Protecao contra malware

Proteção contra Malware envolve o uso de ferramentas e práticas para identificar, bloquear e remover softwares maliciosos que podem prejudicar sistemas, como vírus, ransomware e trojans. Isso inclui o uso de antivírus, firewalls, atualizações de software e educação dos usuários sobre segurança.

Exemplo: Antivírus - Detecta e remove malwares conhecidos, protegendo o sistema de infecções.

Autenticação de dois fatores

O 2FA (Autenticação de dois fatores) é usado para aumentar a segurança no acesso a sistemas e plataformas. Um exemplo de aplicação é a utilização da autenticação de dois fatores em:

Redes sociais – Facebook, Instagram e Twitter oferecem 2FA para evitar acessos indevidos, solicitando um código extra via SMS ou app autenticador.

Ferramentas de gerenciamento de identidade e acesso

Ferramentas de gerenciamento de identidade e acesso (IAM) são essenciais para a segurança cibernética, pois controlam os acessos aos recursos em uma organização. Elas funcionam geralmente através de três componentes principais:

Autenticação:

Verifica a identidade dos usuários.

Autorização:

Determina quais recursos os usuários identificados podem acessar.

Governança de identidade:

É o conjunto de políticas, processos e tecnologias que gerenciam o ciclo de vida das identidades digitais dentro de uma organização. Em suma, é como uma administração centralizada que decide quem tem acesso a quais recursos por quanto tempo.

Alguns benefícios do IAM contam com exemplos:

Segurança aprimorada graças às autenticações de identidade e eficiência operacional na automatização dos processos de acesso.

Exemplos de ferramentas IAM:

Okta identity cloud, Microsoft Azure Active Directory(Azure AD):