STRIDE

A metodologia STRIDE é uma ferramenta usada para identificar possíveis ameaças de segurança em um sistema. É um acrônimo que representa seis categorias diferentes de ameaças: **Spoofing** (Falsificação), **Tampering** (Alteração), **Repudiation** (Repúdio), **Information Disclosure** (Divulgação de Informação**), Denial of Service** (Negação de Serviço) e **Elevation of Privilege** (Elevação de Privilégio). Vamos entender cada uma dessas categorias de forma didática:

1. Spoofing (Falsificação)
- O que é: Falsificação acontece quando alguém se passa por outra pessoa ou sistema para ganhar acesso a informações ou recursos que não deveriam ter. Por exemplo, um atacante pode fingir ser um usuário legítimo para acessar uma conta bancária online.
- Como evitar: Utilizando autenticação forte, como senhas seguras e, de preferência, métodos de autenticação multifator (MFA).

2. Tampering (Alteração)
- O que é: Alteração ocorre quando alguém modifica dados ou código de forma maliciosa. Por exemplo, um invasor pode alterar os registros de um banco de dados para manipular saldos de contas.
- Como evitar: Garantindo a integridade dos dados com o uso de assinaturas digitais, hashing e controles de acesso rigorosos.

3. Repudiation (Repúdio)
- O que é: Repúdio acontece quando uma pessoa nega ter realizado uma ação, como uma transação ou alteração de dados, e não há como provar que ela realmente fez isso. Por exemplo, um cliente pode negar que fez uma compra online, mesmo que ele tenha feito.
- Como evitar: Implementando mecanismos de auditoria e logs detalhados que possam rastrear as ações realizadas no sistema.

4. Information Disclosure (Divulgação de Informação)
- O que é: Divulgação de informação é quando dados confidenciais são expostos a pessoas que não deveriam ter acesso a eles. Isso pode acontecer, por exemplo, quando informações de um cartão de crédito são interceptadas durante uma transação online.
- Como evitar: Criptografando os dados sensíveis tanto em repouso quanto em trânsito, e garantindo que somente usuários autorizados possam acessar essas informações.

5. Denial of Service (Negação de Serviço)
- O que é: Negação de Serviço é um tipo de ataque onde um serviço legítimo é interrompido, tornando-o indisponível para os usuários. Um exemplo clássico é quando um servidor web é sobrecarregado por um grande número de requisições simultâneas, impedindo que usuários legítimos acessem o site.
- Como evitar: Implementando medidas de mitigação, como firewalls, sistemas de detecção de intrusão (IDS) e balanceamento de carga.

6. Elevation of Privilege (Elevação de Privilégio)
- O que é: Elevação de privilégio acontece quando um usuário mal-intencionado consegue obter um nível de acesso mais alto do que deveria. Por exemplo, um usuário comum consegue acesso de administrador e pode alterar configurações críticas do sistema.
- Como evitar: Seguindo o princípio do menor privilégio, onde cada usuário só tem acesso ao que realmente precisa, e implementando controles de acesso fortes e monitoramento contínuo.

Conclusão

A metodologia STRIDE ajuda os desenvolvedores e profissionais de segurança a pensar de forma estruturada sobre as possíveis ameaças aos seus sistemas. Ao considerar cada uma dessas categorias durante o desenvolvimento ou a revisão de um sistema, é possível antecipar riscos e implementar medidas de proteção eficazes.