MicrosoftThreatModelingTechnique

No artigo "A Descriptive Study of Microsoft's Threat Modeling Technique", é realizada uma análise detalhada da metodologia **STRIDE**, desenvolvida pela Microsoft, como uma técnica baseada em modelos para a modelagem de ameaças cibernéticas. As principais componentes e descobertas do estudo incluem:

- **Metodologia STRIDE**:
    - **Desenvolvimento e Propósito**: STRIDE é uma técnica de modelagem de ameaças desenvolvida pela Microsoft que guia o analista de segurança através de várias atividades para identificar e catalogar ameaças que um sistema deve mitigar.
    - **Etapas da Metodologia**:
        1. **Modelagem do Sistema com Diagramas de Fluxo de Dados (DFD)**: Definir o escopo da análise e produzir um modelo do sistema em revisão usando DFDs, que detalham como a informação flui através de sistemas e subsistemas.
        2. **Mapeamento dos Elementos do DFD para Categorias de Ameaças**: As ameaças são organizadas em seis categorias: Spoofing (S), Tampering (T), Repudiation (R), Information Disclosure (I), Denial of Service (D) e Elevation of Privilege (E). Cada tipo de elemento no DFD é suscetível a uma ou mais dessas categorias.
        3. **Elicitação das Ameaças**: Utilização de checklists específicos para cada categoria de ameaça, facilitando a identificação de ameaças concretas que devem ser consideradas no contexto do sistema analisado.
        4. **Documentação das Ameaças**: Embora STRIDE não exija um formato específico, frequentemente são utilizados casos de uso de abuso (misuse cases) para documentar as ameaças, incluindo informações de segurança como pontos de captura para prevenção ou detecção das ameaças.
- **Resultados do Estudo**:
    - **Percepção da Técnica**: A técnica STRIDE não é percebida como difícil de aplicar.
    - **Produtividade**: A produtividade média foi de 1,8 ameaças por hora, indicando um custo de tempo relativamente alto.
    - **Falsos Positivos**: A média de ameaças incorretas foi baixa, correspondendo a 19–24% do total de ameaças produzidas.
    - **Ameaças Omitidas**: A média de ameaças omitidas foi muito alta, correspondendo a 64–69% do total de ameaças identificadas.
    - **Consistência dos Resultados**: As ameaças identificadas estavam mais relacionadas à composição específica das equipes e sua experiência, resultando em resultados inconsistentes.
    - **Comparação com Outras Técnicas**: Métodos como casos de uso de abuso e árvores de ataque mostraram-se mais eficazes na interpretação e análise dos resultados.

Relevância para a Pesquisa

A avaliação da metodologia **STRIDE** apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas, alinhando-se com os objetivos de desenvolver um protocolo que valorize a horizontalidade organizacional como um ativo estratégico. As principais considerações incluem:

- **Eficiência e Produtividade**: A baixa produtividade observada com STRIDE (1,8 ameaças por hora) sugere que, embora a técnica seja acessível para equipes com pouca expertise em segurança, o alto custo de tempo pode ser um impedimento para organizações que operam de forma descentralizada e buscam eficiência na identificação de ameaças.
- **Consistência e Cobertura das Ameaças**: A alta taxa de ameaças omitidas (64–69%) indica uma limitação significativa na capacidade de STRIDE de fornecer uma visão abrangente das ameaças, o que é crucial para estruturas organizacionais horizontais onde a diversidade de operações pode introduzir uma variedade maior de vetores de ataque.
- **Comparação com Outras Metodologias**: A constatação de que métodos alternativos, como casos de uso de abuso e árvores de ataque, oferecem melhores resultados em termos de interpretação e análise, sugere que integrar ou adaptar essas técnicas pode ser benéfico para a criação de um protocolo de modelagem de ameaças mais robusto e confiável.
- **Adaptação às Estruturas Horizontais**: Dado que STRIDE depende fortemente de checklists e categorização padronizada, pode não se adaptar bem a ambientes onde a colaboração e a participação distribuída são essenciais. Métodos que promovem maior criatividade e inclusão de diversas perspectivas, como **Security Cards** e **Persona Non Grata**, podem ser mais adequados para organizações não-hierárquicas.
- **Desenvolvimento de Protocolos Personalizados**: A análise das limitações de STRIDE reforça a necessidade de desenvolver protocolos de modelagem de ameaças que combinem a estrutura e a consistência de STRIDE com a criatividade e a abrangência de outras metodologias. Isso permitirá uma identificação mais completa e eficiente das ameaças, alinhada com a governança horizontal e a confiança distribuída.