

Threat Modeling A Systematic Literature Review

O artigo examina as diversas definições de modelagem de ameaças encontradas na literatura, destacando a multiplicidade e, por vezes, a incompatibilidade dessas definições. Esse estudo visa responder à questão de pesquisa “o que é modelagem de ameaças” e fornecer insights sobre a adoção dessa prática.

Principais Pontos:

1. Diversidade de Definições:

- As definições de modelagem de ameaças são numerosas e utilizadas de maneiras diferentes, possivelmente incompatíveis, conforme identificado na revisão da literatura.
- **Definição Ampla de Uzunov e Fernandez (2014):** “Modelagem de ameaças é um processo que pode ser usado para analisar ataques ou ameaças potenciais, e pode também ser suportado por bibliotecas de ameaças ou taxonomias de ataques”. Esta definição é considerada amplamente aplicável e abrange a análise de ameaças suportada por recursos estruturados.

2. Objetivo da Modelagem de Ameaças:

- A modelagem de ameaças visa entender quais ameaças e ataques os métodos de modelagem pretendem proteger. Isso é essencial para adaptar as metodologias às necessidades específicas das organizações, especialmente aquelas com estruturas não-hierárquicas.
- A classificação das ameaças e ataques é realizada separadamente para diferentes categorias (C1 e C2), com os resultados apresentados em tabelas específicas (Tabela 8 e Tabela 9).

3. Classificação de Ameaças e Ataques:

- **C1 e C2:** As ameaças e ataques são categorizados de forma distinta para cada classe, permitindo uma análise mais detalhada e direcionada.
- **Tabela 8 e Tabela 9:** Apresentam os resultados da classificação, facilitando a compreensão das diferentes tipologias de ameaças abordadas pelos métodos de modelagem de ameaças.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A identificação da diversidade nas definições de modelagem de ameaças reforça a necessidade de um protocolo adaptável, capaz de integrar diferentes perspectivas e abordagens para atender às particularidades das organizações não-hierárquicas.
- **Análise Crítica:** A constatação de que não existe uma definição unificada de modelagem de ameaças incentiva a investigação de métodos que sejam flexíveis e possam ser customizados conforme os requisitos específicos da governança horizontal.
- **Frameworks de Segurança:** A classificação detalhada de ameaças e ataques, conforme apresentada nas tabelas, pode informar o desenvolvimento de frameworks que considerem a complexidade e a diversidade das ameaças enfrentadas por estruturas organizacionais distribuídas.