SoftwareandattackcentricThreatModeling

No artigo "Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment", são avaliadas diversas metodologias de modelagem de ameaças, destacando suas características, vantagens e limitações. As principais metodologias discutidas incluem:

- **Modelagem de Ameaças Centrada em Ativos (Asset Centric Threat Modeling)**:
    - **Descrição**: Envolve uma estratégia de defesa (blue team) focada na proteção da infraestrutura interna de um sistema. É popular em aplicações de tecnologia da informação e negócios, onde ativos como dados de saúde, fundos monetários ou informações pessoalmente identificáveis precisam ser protegidos contra intrusos externos, de forma semelhante a um cofre bancário no domínio físico.
    - **Vantagem**: Foco nas medidas de segurança mais práticas e comprovadas, conforme identificado pelo SANS Institute em 2013, que priorizam as 20 medidas de segurança mais impactantes para a segurança de rede.
    - **Desvantagem**: Limita-se ao domínio cibernético, concentrando-se principalmente na segurança geral de redes, o que pode não abordar ameaças específicas ou emergentes fora desse escopo.
- **DREAD**:
    - **Descrição**: Metodologia de modelagem de ameaças que utiliza um acrônimo para Damage Potential (Potencial de Dano), Reproducibility (Reprodutibilidade), Exploitability (Explorabilidade), Affected Users (Usuários Afetados) e Discoverability (Descobribilidade). Ao invés de usar variáveis booleanas, DREAD adota uma abordagem numérica, atribuindo valores de 0, 5 e 10 para as primeiras quatro categorias e de 0, 5, 9 e 10 para a última, permitindo o cálculo de uma média que representa o risco total do sistema.
    - **Vantagem**: Proporciona uma avaliação quantitativa dos riscos, facilitando a priorização das ameaças com base em pontuações agregadas.
    - **Desvantagem**: A implementação das pontuações pode ser subjetiva e inconsistente, afetando a confiabilidade das avaliações de risco.
- **TRIKE**:
    - **Descrição**: Framework de modelagem de ameaças de código aberto que se assemelha às metodologias da Microsoft, como STRIDE e DREAD, mas com foco em uma abordagem baseada em risco. TRIKE enfatiza o impacto sobre os stakeholders do sistema, ao invés de apenas categorizar ataques, ameaças e vulnerabilidades.
    - **Vantagem**: Oferece uma perspectiva orientada a riscos, considerando o impacto direto nas partes interessadas, o que pode resultar em uma análise de ameaças mais alinhada com os objetivos de negócios.
    - **Desvantagem**: A abordagem baseada em risco pode ser mais complexa e exigir um entendimento mais profundo dos impactos, tornando a implementação mais trabalhosa.
- **PASTA (Process for Attack Simulation and Threat Analysis)**:

- **Descrição**: Desenvolvido por Uceda Velez et al., PASTA é um framework de modelagem de ameaças que consiste em 7 camadas, oferecendo capacidades de modelagem mais detalhadas do que as ferramentas tradicionais. PASTA foca em simular ataques e analisar ameaças viáveis para um alvo de aplicação específico.
- **Vantagem**: Proporciona uma modelagem de ameaças mais abrangente e detalhada, permitindo uma análise aprofundada das ameaças e suas potenciais consequências.
- **Desvantagem**: O processo extensivo com várias camadas de modelagem pode ser demorado e complexo, exigindo mais recursos e expertise para sua implementação eficaz.

Relevância para a Pesquisa

A avaliação das metodologias **Asset Centric Threat Modeling**, **DREAD**, **TRIKE** e **PASTA** é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**, alinhando-se diretamente com o objetivo de desenvolver um protocolo que valorize a **horizontalidade organizacional** como um ativo estratégico. As principais considerações incluem:

- **Adaptação às Estruturas Horizontais**:
    - **PASTA** e **TRIKE**, com suas abordagens detalhadas e baseadas em risco, oferecem uma modelagem de ameaças mais alinhada com a necessidade de compreensão profunda das interações e impactos nas organizações descentralizadas.
    - **DREAD**, embora forneça uma avaliação quantitativa, pode necessitar de adaptações para garantir consistência e reduzir a subjetividade nas pontuações, garantindo que a avaliação de riscos seja confiável e aplicável em estruturas horizontais.
- **Equilíbrio entre Consistência e Abrangência**:
    - **Asset Centric Threat Modeling** foca nas medidas de segurança mais práticas e comprovadas, o que pode ser útil para estabelecer uma base consistente de segurança em organizações distribuídas.
    - **PASTA**, com sua modelagem detalhada, complementa a necessidade de identificar ameaças complexas e multifacetadas que são comuns em ambientes organizacionais não-hierárquicos.
- **Flexibilidade e Adaptabilidade**:
    - A natureza extensiva de **PASTA** permite uma adaptação flexível às necessidades específicas de organizações horizontais, onde a colaboração e a distribuição de responsabilidades são essenciais.
    - **TRIKE**, com seu enfoque em impacto sobre stakeholders, facilita uma abordagem mais personalizada e contextualizada na identificação e mitigação de ameaças, refletindo melhor a dinâmica das organizações não-hierárquicas.
- **Consistência e Redução de Falsos Positivos**:
    - **DREAD** pode enfrentar desafios na consistência das avaliações devido à subjetividade das pontuações, o que pode ser mitigado através de treinamentos e padronizações específicas para ambientes horizontais.

    - **Asset Centric Threat Modeling** e **PASTA** oferecem abordagens que, embora mais complexas, podem proporcionar uma maior consistência e cobertura abrangente das ameaças, minimizando a ocorrência de falsos positivos e assegurando uma identificação mais completa dos riscos.
- **Integração com Outras Metodologias**:
    - A combinação de **PASTA** com outras abordagens mais criativas e colaborativas, como **Security Cards** e **Persona Non Grata**, pode resultar em um protocolo de modelagem de ameaças mais robusto e adaptável, atendendo às especificidades das organizações não-hierárquicas.
    - **TRIKE** e **DREAD** podem ser integrados para fornecer uma avaliação quantitativa complementar à modelagem detalhada de ameaças, oferecendo uma visão mais holística e multifacetada dos riscos.