RiskCentricThreatModeling

Resumo da Anotação

No artigo "Risk Centric Threat Modeling Process for Attack Simulation and Threat Analysis", é apresentada uma metodologia centrada em riscos para a modelagem de ameaças, denominada PASTA (Process for Attack Simulation and Threat Analysis). As principais ideias e componentes abordados no texto incluem:

- **Importância de um Processo de Segurança Eficaz**:
    - Um processo de segurança bem-sucedido deve ser repetível, mensurável, produzir resultados e envolver múltiplas partes interessadas além das áreas tradicionais de segurança e conformidade.
    - A metodologia PASTA oferece um método linear que aborda esses requisitos, facilitando a integração de diversos stakeholders no processo de modelagem de ameaças.
- **Desafios Inerentes à Modelagem de Ameaças**:
    - Cultura organizacional, recursos disponíveis, maturidade dos processos e controles, e suporte executivo são desafios significativos.
    - PASTA promove coesão entre grupos de segurança em operações, governança, arquitetura e desenvolvimento, mitigando esses desafios.
- **Benefícios da Metodologia PASTA**:
    - **Cohesão entre Grupos de Segurança**: Facilita a colaboração entre diferentes departamentos, como operações, governança, arquitetura e desenvolvimento.
    - **Economia de Recursos**: Ao incorporar a governança de segurança no início dos esforços de desenvolvimento, reduz lacunas de conformidade, descobertas de auditoria e questões de risco.
    - **Compreensão Aprofundada das Fontes de Ataque**: Evita o uso de scripts de ataque prefabricados, promovendo uma compreensão mais detalhada das vulnerabilidades e como os ataques realmente exploram essas fraquezas.
    - **Treinamento e Conscientização em Segurança**: Integra princípios de segurança no fluxo de trabalho normal do SDLC, melhorando a compreensão dos desenvolvedores e outros profissionais sobre como a inação em medidas corretivas pode introduzir riscos.
    - **Abordagem Colaborativa**: Reduz a mentalidade adversarial entre equipes de segurança e outras áreas, promovendo uma colaboração mais harmoniosa.
- **Componentes do Processo PASTA**:
    - **Stage I: Definição dos Objetivos (DO)**: Derivação de requisitos de segurança e conformidade, determinação dos impactos de negócios e perfil de risco.
    - **Stage II: Definição do Escopo Técnico (DTS)**: Enumeração de detalhes técnicos, incluindo usuários, contas funcionais, componentes de software e infraestrutura de terceiros.
    - **Stage III: Decomposição e Análise da Aplicação (ADA)**: Decomposição da aplicação em elementos funcionais básicos, tipos de usuários, dados acessados e controles de segurança.

    - **Stage IV: Análise de Ameaças (TA)**: Identificação e análise de ameaças específicas contra os componentes e ativos da aplicação.
    - **Stage V: Análise de Fraquezas e Vulnerabilidades (WVA)**: Associação de ameaças com vulnerabilidades previamente identificadas e análise das fraquezas nos controles de segurança.
    - **Stage VI: Modelagem e Simulação de Ataques (AMS)**: Análise de cenários de ataque para determinar a probabilidade e impactos técnicos, utilizando árvores de ataque para identificar os caminhos de ataque mais prováveis.
    - **Stage VII: Análise e Gestão de Riscos (RAM)**: Identificação dos impactos técnicos e de negócios, e determinação das medidas de segurança para mitigar os riscos identificados.
- **Uso de Árvores de Ataque**:
    - As árvores de ataque são utilizadas para aprender sobre os objetivos e métodos dos atacantes, determinando caminhos de menor resistência e custo, aumentando a probabilidade de execução e dano à aplicação.
    - A construção de casos de teste de simulação de ataques permite verificar a eficácia das medidas de segurança preventivas e detectivas implementadas.

Relevância para a Pesquisa

A metodologia PASTA apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. Sua abordagem centrada em riscos e estrutura linear facilita a criação de um protocolo de modelagem de ameaças que considera a horizontalidade organizacional como um ativo estratégico. Especificamente:

- **Integração de Stakeholders**: PASTA promove a colaboração entre diversas áreas da organização, alinhando-se com a necessidade de estruturas horizontais que valorizam a participação distribuída e a confiança compartilhada.
- **Avaliação Abrangente de Riscos**: A abordagem detalhada de PASTA para identificar e analisar ameaças e vulnerabilidades permite uma compreensão aprofundada das nuances específicas das organizações descentralizadas, onde os vetores de ataque podem ser mais variados e complexos.
- **Uso de Árvores de Ataque**: A aplicação de árvores de ataque dentro do PASTA facilita a representação estruturada das ameaças, permitindo uma análise sistemática e a identificação de caminhos de ataque que consideram a distribuição de responsabilidades e a ausência de uma hierarquia rígida.
- **Escalabilidade e Adaptabilidade**: A metodologia PASTA, com seus estágios bem definidos, suporta a escalabilidade necessária para organizações distribuídas e a adaptabilidade para incorporar novas ameaças e mudanças organizacionais, essenciais para manter a segurança em ambientes dinâmicos.
- **Treinamento e Conscientização**: Ao integrar princípios de segurança no fluxo de trabalho normal, PASTA contribui para a construção de uma cultura de segurança distribuída, onde todos

os membros da organização estão conscientes e engajados na mitigação de riscos, reforçando a governança horizontal.

Portanto, a aplicação da metodologia PASTA na modelagem de ameaças proporciona uma base robusta para desenvolver um protocolo que valorize a estrutura horizontal das organizações, promovendo uma abordagem colaborativa e abrangente para a segurança cibernética. Isso está diretamente alinhado com os objetivos específicos da pesquisa de criar um protocolo que utilize a horizontalidade como um ativo estratégico, além de apoiar a análise de modelos de governança, confiança distribuída e frameworks de segurança.