SecurityCardsToolkit

No documento "A Security Threat Brainstorming Toolkit", são apresentados recursos e atividades destinados a facilitar a identificação e análise de ameaças de segurança em sistemas tecnológicos. As principais componentes abordadas incluem:

- **Títulos das Cartas (Card Titles)**:
    - **Motivações do Adversário**:
        - Acesso ou Conveniência
        - Curiosidade ou Tédio
        - Desejo ou Obsessão
        - Diplomacia ou Guerra
        - Maldade ou Vingança
        - Dinheiro
        - Política
        - Proteção
        - Religião
        - Auto-Promoção
        - Visão de Mundo
        - Motivações Incomuns
    - **Recursos do Adversário**:
        - Expertise (Especialização)
        - Um Mundo Futuro
        - Impunidade
        - Capacidades Internas
        - Conhecimento Interno
        - Dinheiro
        - Poder e Influência
        - Tempo
        - Ferramentas
        - Recursos Incomuns
    - **Métodos do Adversário**:
        - Encobrimento de Ataque
        - Ataque Indireto
        - Manipulação ou Coerção
        - Ataque em Múltiplas Fases
        - Ataque Físico
        - Processos
        - Ataque Tecnológico
        - Métodos Incomuns
    - **Impacto Humano**:
        - A Biósfera
        - Bem-Estar Emocional
        - Bem-Estar Financeiro

        - Dados Pessoais
        - Bem-Estar Físico
        - Relacionamentos
        - Bem-Estar Social
        - Impactos Incomuns
- **Exemplo de Atividade**:
    - Trabalhar em grupos de 3-5 pessoas.
    - Considerar um sistema tecnológico exemplo ou um sistema que está sendo projetado.
    - Percorrer o baralho de cartas e familiarizar-se com as dimensões e as cartas. Garantir a leitura de pelo menos uma carta de cada dimensão na íntegra.
    - Dentro de cada dimensão, classificar as cartas em ordem de relevância para o sistema e o nível de risco que elas apresentam.
    - Justificar a classificação das cartas nessa ordem.
    - Identificar cenários de ataque específicos que surgiram. Perfis de atacantes particulares começam a emergir?
- **Recursos Adicionais**:
    - Writeups completos e outras atividades estão disponíveis em securitycards.cs.washington.edu.

Relevância para a Pesquisa

A utilização de um **Security Threat Brainstorming Toolkit**, como apresentado no artigo, é altamente relevante para a modelagem de ameaças em organizações não-hierárquicas, conforme os objetivos da pesquisa. Este toolkit oferece uma abordagem estruturada e colaborativa para identificar e categorizar potenciais ameaças, o que é essencial em ambientes onde a governança e a responsabilidade são distribuídas de forma horizontal. Especificamente:

- **Facilitação da Colaboração Distribuída**: A atividade de brainstorming em grupo promove a participação de múltiplos stakeholders, alinhando-se com a estrutura não-hierárquica das organizações focadas na pesquisa. Isso permite a inclusão de diversas perspectivas na identificação de ameaças, reforçando a confiança distribuída.
- **Identificação Abrangente de Vetores de Ataque**: As categorias de motivações, recursos e métodos dos adversários, bem como os impactos humanos, fornecem um quadro detalhado para a análise de ameaças. Isso é particularmente útil para organizações horizontais, onde as ameaças podem ser variadas e complexas, exigindo uma abordagem multifacetada para a modelagem de riscos.
- **Flexibilidade e Adaptabilidade**: O uso de cartas permite que a equipe de modelagem de ameaças adapte e personalize a identificação de riscos conforme as especificidades do sistema ou projeto em questão. Esta flexibilidade é crucial para organizações descentralizadas que operam em contextos dinâmicos e em constante evolução.
- **Melhoria da Consistência e Profundidade na Análise de Ameaças**: Ao seguir uma metodologia padronizada de classificação e justificativa das ameaças, o toolkit ajuda a assegurar

que todas as áreas relevantes sejam consideradas, aumentando a consistência e a profundidade dos modelos de ameaça desenvolvidos. Isso contribui para a criação de protocolos de segurança mais robustos e abrangentes.

- **Desenvolvimento de Cenários de Ataque Realistas**: A identificação de perfis de atacantes e cenários de ataque emergentes a partir das atividades propostas permite a criação de modelos de ameaça que refletem melhor as possíveis realidades enfrentadas pelas organizações. Isso é alinhado com o objetivo de desenvolver um protocolo que considere a horizontalidade como um ativo estratégico, garantindo que as contramedidas sejam eficazes e contextualizadas.