KeepingAheadofOurAdversaries

No artigo "Keeping Ahead of Our Adversaries", são discutidas abordagens para a modelagem de ameaças de segurança em sistemas tecnológicos, com ênfase na utilização do **Security Cards**, um toolkit de brainstorming desenvolvido por Tamara Denning, Batya Friedman e Tadayoshi Kohno. As principais ideias e componentes abordados no texto incluem:

- **Objetivos da Modelagem de Ameaças**:
    - **Identificar Capacidades e Objetivos dos Atacantes**: Compreender as habilidades e metas dos adversários para catalogar ameaças potenciais que o sistema deve mitigar.
    - **Atividade de Requisitos**: A modelagem de ameaças é considerada uma atividade de requisitos, onde a compreensão das necessidades de segurança é essencial para o desenvolvimento de requisitos completos e consistentes.
- **Security Cards: Um Toolkit de Brainstorming para Ameaças de Segurança**:
    - **Estrutura do Toolkit**:
        - **Total de Cartas**: 42 cartas divididas em quatro dimensões principais:
            1. **Impacto Humano (Human Impact)**: Explora como violações de segurança podem afetar os indivíduos e a sociedade, incluindo privacidade pessoal, bem-estar emocional e físico, bem-estar financeiro, relacionamentos e impactos incomuns.
            2. **Motivações do Adversário (Adversary's Motivations)**: Descreve os motivos que levam alguém a atacar um sistema, como malícia, vingança, promoção pessoal, diplomacia ou guerra, entre outros.
            3. **Recursos do Adversário (Adversary's Resources)**: Analisa os ativos que um adversário pode utilizar para lançar um ataque, incluindo ferramentas de hardware e software, expertise técnica, impunidade, conhecimento interno, dinheiro, poder e influência, tempo e recursos incomuns.
            4. **Métodos do Adversário (Adversary's Methods)**: Explora as abordagens de alto nível que um adversário pode utilizar para realizar um ataque, como manipulação de pessoas, ataques indiretos, coerção, ataques multifase, ataques físicos e tecnológicos, entre outros.
    - **Objetivos da Metodologia**:
        - **Categorizar e Avaliar Vulnerabilidades**: Fornece uma maneira prática de categorizar e avaliar as vulnerabilidades de sistemas de coleta e gestão de identidade.
        - **Estimular Pensamento Criativo e Abrangente**: Promove a identificação de ataques incomuns ou sofisticados, ajudando desenvolvedores e mantenedores a antecipar ameaças não previstas por abordagens tradicionais.
        - **Compreensão de Técnicas de Ataque**: Facilita a compreensão das técnicas e padrões de ataque já utilizados e postula aqueles que podem ser tentados no futuro, permitindo a antecipação de ameaças emergentes.

- **Exemplo de Aplicação das Security Cards**:
    - **Contexto**: Aplicação das Security Cards a um Sistema de ICD (Implantable Cardioverter Defibrillator).
    - **Dimensões e Exemplos de Cartas**:
        - **Impacto Humano**:
            1. **Bem-Estar Físico**: Avaliar como um ICD comprometido pode impactar a saúde física dos usuários.
            2. **Bem-Estar Emocional**: Considerar como os pacientes podem se sentir ameaçados à sua saúde.
            3. **Bem-Estar Financeiro e Relacionamentos**: Analisar como um ataque pode descreditar a empresa responsável pelo ICD ou comprometer dados pessoais.
            4. **Dados Pessoais**: Explorar como informações identificadoras armazenadas no dispositivo podem ser usadas por atacantes.
        - **Motivações do Adversário**:
            1. **Malícia ou Vingança**: Atacantes podem visar usuários de ICD por emoções extremas.
            2. **Promoção Pessoal**: Atacantes podem querer demonstrar habilidades técnicas.
            3. **Diplomacia ou Guerra**: Atacantes podem visar inimigos políticos que possuem ICDs.
        - **Recursos do Adversário**:
            1. **Expertise Técnica**: Avaliar as habilidades técnicas dos hackers.
            2. **Impunidade**: Considerar a dificuldade de responsabilizar ou processar o atacante.
            3. **Conhecimento Interno**: Explorar como ex-funcionários com conhecimento detalhado da arquitetura podem comprometer o sistema.
        - **Métodos do Adversário**:
            1. **Ataque Tecnológico**: Utilizar métodos tecnológicos para comprometer o ICD.
            2. **Ataque Multifase**: Alterar o software em escritórios médicos responsáveis pelo envio de comandos ao ICD.
            3. **Ataque Indireto e Encobrimento**: Manipular processos burocráticos ou esconder a origem do ataque.
- **Transição de Ameaças para Requisitos**:
    - **Exemplo de Ameaça**: "Como um especialista em TI com intenção de prejudicar fisicamente um paciente com ICD, lançarei um ataque no dispositivo que alterará os efeitos pretendidos no coração do paciente."
    - **Aplicação**: Utilizar a catalogação de ameaças para melhorar o software em desenvolvimento, transformando ameaças identificadas em requisitos de segurança específicos para mitigar os riscos.

Relevância para a Pesquisa

A utilização do **Security Threat Brainstorming Toolkit**, conforme apresentado no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. 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:

- **Abordagem Estruturada e Colaborativa**: O uso das **Security Cards** facilita a colaboração entre diversos stakeholders, promovendo uma participação distribuída que é característica das estruturas horizontais. Isso reforça a confiança distribuída e a governança horizontal, elementos centrais na segurança organizacional em ambientes descentralizados.
- **Identificação Abrangente de Vetores de Ataque**: As quatro dimensões das cartas permitem uma análise detalhada e multifacetada das possíveis ameaças, assegurando que aspectos como impacto humano, motivações, recursos e métodos dos adversários sejam considerados de forma holística. Isso é crucial para organizações não-hierárquicas, onde as ameaças podem ser mais diversificadas e complexas, exigindo uma abordagem multifacetada para a modelagem de riscos.
- **Estimulação de Pensamento Criativo**: Ao incentivar o pensamento criativo e abrangente sobre ameaças, o toolkit ajuda a identificar vetores de ataque que poderiam passar despercebidos em abordagens mais tradicionais. Isso é especialmente importante em estruturas horizontais, onde a distribuição de responsabilidades pode introduzir novas vulnerabilidades.
- **Flexibilidade e Adaptabilidade**: A metodologia das **Security Cards** é flexível e adaptável, permitindo que as organizações ajustem a identificação de ameaças conforme suas necessidades específicas e contextos operacionais. Essa adaptabilidade é essencial para organizações descentralizadas que operam em ambientes dinâmicos e em constante evolução.
- **Melhoria na Consistência e Profundidade dos Modelos de Ameaça**: Ao seguir uma metodologia padronizada para categorizar e avaliar ameaças, as **Security Cards** asseguram uma maior consistência e profundidade na análise de riscos. Isso contribui para a criação de modelos de ameaça mais robustos e confiáveis, fundamentais para a segurança em estruturas organizacionais horizontais.
- **Desenvolvimento de Contramedidas Eficazes**: A identificação sistemática das ameaças facilita a implementação de contramedidas eficazes e contextualizadas, alinhadas com a distribuição de responsabilidades e a ausência de uma hierarquia rígida. Isso garante que as medidas de segurança sejam apropriadas e eficazes para mitigar os riscos identificados.