SecurityDevelopmentLifecycle

No eBook "The Security Development Lifecycle" da Microsoft, é discutida a importância e os detalhes do processo de **modelagem de ameaças** como uma atividade crucial no ciclo de vida de desenvolvimento de software. As principais ideias abordadas no trecho fornecido incluem:

- **Importância da Modelagem de Ameaças**:
    - **Prioridade na Segurança**: Se fosse possível escolher apenas uma ação para melhorar a segurança do software – modelagem de ameaças, revisões de código de segurança ou testes de segurança – a modelagem de ameaças seria a escolhida, devido à sua capacidade de identificar problemas de segurança no início do ciclo de desenvolvimento.
    - **Economia de Custos**: Resolver questões de segurança precocemente resulta em significativas economias de custos, pois as correções são mais baratas e menos disruptivas quando feitas nas fases iniciais do desenvolvimento.
- **Benefícios da Modelagem de Ameaças**:
    - **Contribuição para o Gerenciamento de Riscos**: As ameaças identificadas são riscos tanto para os usuários quanto para o ambiente que implementa o software.
    - **Detecção Precoce de Ameaças**: Identificar ameaças antes que o sistema seja codificado permite a resolução de problemas de design de segurança de forma proativa.
    - **Revalidação da Arquitetura e Design**: Revisar o design com foco em segurança e privacidade reforça a robustez do sistema.
    - **Perspectiva Diferente**: Força a equipe de desenvolvimento a considerar o design sob a ótica da segurança e privacidade, focando nos componentes com alta probabilidade de ataque.
    - **Seleção de Contramedidas Adequadas**: Auxilia na escolha das contramedidas apropriadas para o aplicativo e seu ambiente.
    - **Redução da Superfície de Ataque**: Contribui para a redução das áreas vulneráveis do software.
    - **Guia para Revisões de Código e Testes de Penetração**: Orienta processos de revisão de código e testes de penetração, aumentando a eficácia das análises de segurança.
- **Produção e Utilização dos Modelos de Ameaças**:
    - **Documentação**: O principal resultado do processo de modelagem de ameaças é um documento que descreve informações de fundo sobre a aplicação, define o modelo de alto nível (geralmente usando Diagramas de Fluxo de Dados - DFDs), lista os ativos que precisam ser protegidos e as ameaças ao sistema.
    - **Modelagem Modular**: Para sistemas grandes, é mais eficiente modelar módulos menores, mas isso pode levar a lacunas de segurança na composição final do sistema.
    - **Definição de Fronteiras de Confiança**: Identificar fronteiras de confiança ajuda a determinar onde os dados mudam de um nível de privilégio para outro, permitindo a análise de segurança nesses pontos críticos.
- **Processo de Modelagem de Ameaças com STRIDE**:
    - **Etapas da Metodologia STRIDE**:

1. **Definir Cenários de Uso**: Identificar como os usuários interagem com o sistema.
2. **Coletar Dependências Externas**: Listar todos os componentes externos que o sistema utiliza.
3. **Definir Assunções de Segurança**: Estabelecer suposições sobre a segurança do sistema.
4. **Criar Notas de Segurança Externas**: Documentar considerações de segurança externas ao sistema.
5. **Criar DFDs**: Desenvolver Diagramas de Fluxo de Dados para modelar o sistema.
6. **Determinar Tipos de Ameaças**: Categorizar as ameaças conforme o modelo STRIDE.
7. **Identificar Ameaças ao Sistema**: Listar ameaças específicas com base nos DFDs.
8. **Determinar Risco**: Avaliar o nível de risco associado a cada ameaça.
9. **Planejar Mitigações**: Desenvolver estratégias para mitigar os riscos identificados.

- **Descobertas do Estudo**:
    - **Percepção da Técnica STRIDE**: A técnica STRIDE não é considerada difícil de aplicar.
    - **Produtividade**: A produtividade média foi de 1,8 ameaças por hora, indicando um custo de tempo relativamente alto.
    - **Falsos Positivos**: A média de ameaças incorretas foi baixa, correspondendo a 19–24% do total de ameaças produzidas.
    - **Ameaças Omitidas**: A média de ameaças omitidas foi muito alta, correspondendo a 64–69% do total de ameaças identificadas.
    - **Consistência dos Resultados**: As ameaças identificadas estavam mais relacionadas à composição específica das equipes e sua experiência, resultando em resultados inconsistentes.
    - **Comparação com Outras Técnicas**: Métodos como casos de uso de abuso e árvores de ataque mostraram-se mais eficazes na interpretação e análise dos resultados.

Relevância para a Pesquisa

A análise da metodologia **STRIDE** apresentada no eBook da Microsoft é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**. As principais considerações incluem:

- **Eficiência e Custo de Tempo**: A produtividade relativamente baixa observada com STRIDE (1,8 ameaças por hora) sugere que, embora a técnica seja acessível para equipes com pouca expertise em segurança, o alto custo de tempo pode ser um impedimento para organizações que operam de forma descentralizada e buscam eficiência na identificação de ameaças.
- **Cobertura de Ameaças**: A alta taxa de ameaças omitidas (64–69%) indica que STRIDE pode não ser suficientemente abrangente para capturar todas as ameaças relevantes em ambientes

organizacionais horizontais, onde a diversidade de operações pode introduzir uma variedade maior de vetores de ataque.

- **Consistência dos Resultados**: A inconsistência dos resultados de STRIDE, devido à variação na composição e experiência das equipes, destaca a necessidade de metodologias que ofereçam uma identificação mais padronizada e abrangente das ameaças, especialmente em estruturas organizacionais distribuídas.
- **Comparação com Outras Metodologias**: A constatação de que métodos alternativos, como casos de uso de abuso e árvores de ataque, oferecem melhores resultados em termos de interpretação e análise, sugere que a integração dessas técnicas pode ser benéfica para a criação de um protocolo de modelagem de ameaças mais robusto e confiável.
- **Adaptação às Estruturas Horizontais**: Considerando que STRIDE depende fortemente de checklists e categorização padronizada, pode não se adaptar bem a ambientes onde a colaboração e a participação distribuída são essenciais. Métodos que promovem maior criatividade e inclusão de diversas perspectivas, como **Security Cards** e **Persona Non Grata**, podem ser mais adequados para organizações não-hierárquicas.
- **Desenvolvimento de Protocolos Personalizados**: A análise das limitações de STRIDE reforça a necessidade de desenvolver protocolos de modelagem de ameaças que combinem a estrutura e a consistência de STRIDE com a criatividade e a abrangência de outras metodologias. Isso permitirá uma identificação mais completa e eficiente das ameaças, alinhada com a governança horizontal e a confiança distribuída.
- **Foco na Consistência e Completude**: A alta taxa de ameaças omitidas em STRIDE destaca a importância de garantir que o protocolo de modelagem de ameaças desenvolvido para organizações horizontais seja capaz de identificar uma ampla gama de ameaças de maneira consistente, evitando vulnerabilidades que podem ser exploradas em ambientes onde a supervisão centralizada é mínima.