Aula 06 → Modelagem de Ameaças

Modelgagem de ameaças

- Abordagem estruturada;
- Identifica e mensura riscos associados ao software;
- Permite que o design enderece os riscos de segurança
- Define os requisistos recursos de segurança;
- Ajuda a revisar testes e revisões de código.

Conceitos Básicos

- **Ativos** → recursos de valor, alvo do atacando (dados do BD, dados de arquivos).
- **Ameaças** → ocorrência potencial que pode comprometer recursos (ativo + vulnera. + atacante)
- **Agentes de Ameaça** → ator que executa o ataque, com motivações próprias.
- **Vulnerabilidades** → pontos fracos, recursos que tornam uma ameaça possível.
- **Ataque** → ação que prejudica o recurso, ato de explorar a vulnerabilidade.
- **Controle** → trata a ameaça, reduzindo o risco

Processo

1. **Identificar os bens;**
    - Identificar recursos à proteger;

2. **Criar um panorama de arquitetura;**
    - Identificar o que a aplicação faz;
    - Crirar um diagrama da arquitetura
    - Identificar as tecnologias

3. **Decompor o Software;**
    - Revelar as vulnerabilidades
    - Identificar limites de confiaça: fluxo de dados, limites de entrada…

4. **Identificar ameaças;**
    - Pode-se usar o modelo **STRIDE**, simples sem detalhes.

      Spoofing → falsificação

      Tampering → violação alteração

      Repudiation → sem responsabilização adequada

      Information Disclosure → vazamento de informações

      Denial of Service → negação de serviço

Elevation of Privilege → elevação de privilégio

- Exemplo:

Ativo	S	T	R	I	D	E
Entidade Externa	X		X			
Processo		X		X	X	X
Repositório		X		X	X	
Fluxo de Dados		X		X	X	

5. **Documentar ameaças;**
   - Anotar informações como: alvo da ameaça, risco, ataque, controle
   - Exemplo:

Descrição da Ameaça	O invasor obtém credencias de autenticação monitorando a rede.
Ativo (alvo da ameaça)	Processo de autenticação de usuário da aplicação
Risco	Médio
Ataque	Uso do software de monitoramento da rede
Controle	Uso do SSL para fornecer canal criptografado

6. **Classificar ameaças.**
   - Considerar a probabilidade dos danos que poderiam causar num caso de ataque.
   - Grave, Média, Pequena → comparar riscos com investimentos necessários.
   - Pode-se usar o método DREAD
   - Exemplo: Risco MÉDIO → 10 pts

SILGA	Classificação	Alto (3)	Médio (2)	Baixo (1)
D	Danos em Potencial	X		
R	Reprodutibilidade	X		
E	Explorabilidade			X
A	Usuários Afetados		X	
D	Possibilidade de Descobrimento			X

Somar os pontos de cada letra e classificar a ameaça:

5 → 7: Pequeno

8 → 11: Médio

12 → 15: Grave