



Requisitos de segurança

Derivação de controles a partir das ameaças modeladas

Derivação de requisitos

O modelo de ameaças

O modelo de ameaças é o motor do processo de derivação de requisitos.

O modelo define um “problema” que é endereçado por um requisito de segurança, também chamado de controle, que visa “resolver” aquele problema.

Os requisitos derivados

A prática de Requisitos de Segurança (SR) está focada em especificar claramente o comportamento esperado do software em relação à segurança.

Como marco final desta disciplina buscase a garantia de que os requisitos de segurança sejam implementados e testados, mediante as entregas dos projetos, para garantir que o “problema” claramente identificado no modelo de ameaças seja de fato sanado pelo requisito.

Nota: Definir requisitos baseados em “melhores práticas” sem analisar a ameaça causa muito desperdício de recursos e aumenta a complexidade dos sistemas.

Derivação de requisitos

Resultados de uma derivação clara de requisitos

1. Alinhamento do esforço de desenvolvimento com os riscos do negócio
2. Adoção das melhores práticas da indústria para segurança de requisitos explícitos
3. Conscientização das medidas adotadas para mitigar o riscos de segurança por todo o time do projeto
4. Conhecimento detalhado dos cenários de ataque contra a lógica de negócios
5. Priorização de desenvolvimento para recursos de segurança com base em ataques prováveis
6. Tomada de decisão fundamentada sobre esforços de segurança/aceite de risco
7. Avaliação/revisão clara de requisitos funcionais que apresentem falhas de segurança
8. Controle do esforço de segurança realizado em cada equipe de projeto

Direta ou indiretamente todos os resultados-alvo de quem objetiva adotar boas práticas de “Requisitos de Segurança” implicam na adoção casada da modelagem de ameaças, seja pelo esclarecimento das necessidade, seja pela priorização dos ataques mais prováveis, seja pela tomada de decisão sobre aceite de risco de forma realmente fundamentada.