9.2 Progettazione di applicazioni sicure

Le azioni di sicurezza di questa fase possono essere così sintetizzate:

- **Analisi e modellazione delle minacce**, attraverso l'identificazione dei componenti applicativi coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema;
- **Analisi della superficie d'attacco e della finestra di opportunità,** allo scopo di individuare le parti del sistema che possono essere esposte ad attacchi e pertanto lo rendono vulnerabile;
- **Piano di mitigation,** attraverso l'identificazione delle contromisure da adottare in questa fase al fine di mitigare le potenziali minacce individuate (utilizzando anche tool automatici e semiautomatici);
- **Secure Design Refactoring**, revisione progettuale che attua le contromisure individuate; produzione di un High Level Design conforme ai principi del Secure by Design;
- Questa fase produce come output finale la Reportistica/documentazione completa che sintetizza i risultati per ogni punto precedente (Specifiche Software comprensive delle contromisure).

Questa fase è inoltre responsabile della revisione dei requisiti di sicurezza individuate nella fase precedente di definizione dei requisiti di sicurezza (paragrafo 9.1).

La figura che segue sintetizza gli elementi in input e l'output prodotto dal processo di Progettazione di software sicuro:

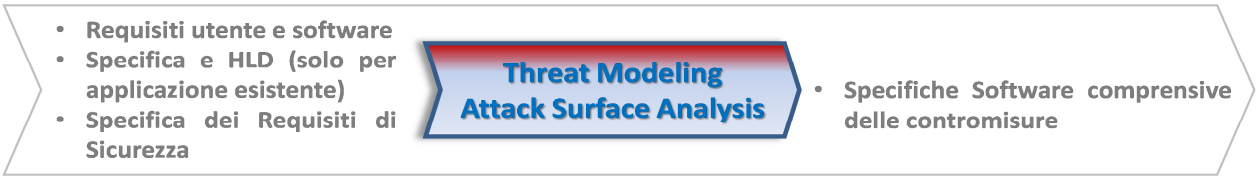

Figura 19 - Input e Output della fase Threat Modeling Attack Surface Analysis

Le linee guida di progettazione sicura sono oggetto del documento ***Allegato 4 - Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design***. Si rinvia a quest'ultimo per ulteriori dettagli della metodologia da adottare.

9.2.1 Identificazione degli strumenti a supporto

Dopo aver identificato e documentato le esigenze di sicurezza, viene eseguita la modellazione delle minacce col fine di riconoscere e assegnare delle priorità a queste ed individuare le opportune contromisure per la loro mitigazione. A differenza delle tecniche di verifica, come ad esempio il penetration testing, il modello di minacce ottenuto attraverso la relativa modellazione, deve essere eseguito prima che un prodotto o un servizio venga implementato. Questo contribuisce a realizzare un prodotto finale più sicuro indirizzando problematiche di sicurezza ad un early-stage del ciclo di sviluppo. Il processo per la costruzione di un modello di minacce consiste dei seguenti step:

- Disegno dell'architettura del sistema;
- Individuazione dei confini di fiducia;
- Identificazione delle minacce;
- Individuazione delle contromisure da attuare per mitigare le minacce;
- Eventuale riprogettazione dei componenti per mitigare le minacce;