La modellazione delle minacce è una parte importante del ciclo di vita del software che identifica le minacce che potrebbero non essere riconosciute nelle tradizionali sessioni di brainstorming sulla sicurezza.
A differenza delle tecniche di test del software come il penetration testing o fuzzing, la modellazione delle minacce può essere eseguita durante la fase di progettazione del sistema rendendola totalmente indipendente dallo sviluppo del codice. Introdotto nel ciclo di vita dello sviluppo del software, il Threat Modeling può significativamente contribuire a garantire la sicurezza già nella fase di progettazione e disegno di un'applicazione, riducendo i costi e minimizzando le necessarie successive correzioni di sicurezza nel progetto. Anche i sistemi in essere possono beneficiare di tale processo. Possono essere identificate nel sistema le difettosità di sicurezza sconosciute o non risolte e può essere applicata una classificazione del rischio alle vulnerabilità individuate. Questo processo può anche essere adattato alle pratiche di sviluppo come Agile.

5.5.2 Motivazioni nell'uso del Threat Model

5.5.2.1 Ricerca preventiva dei bug di sicurezza

Si pensi alla costruzione di una casa; le decisioni prese all'inizio del progetto impatteranno drasticamente sulla sicurezza del prodotto finale. La scelta di pareti di legno e un consistente numero di finestre al piano terra, espongono la casa a maggiori rischi rispetto a una costruzione fatta in mattoni e con poche finestre. A seconda di dove si sta costruendo e di altri fattori, potrebbe anche essere una scelta ragionevole. Comunque, una volta effettuata la scelta, possibili futuri cambiamenti avrebbero sicuramente un impatto significativo sui costi. Certo, si possono sempre mettere delle inferriate sulle finestre, ma non sarebbe meglio concepire una soluzione più efficace e appropriata sin dall'inizio? È possibile applicare gli stessi tipi di compromessi alla tecnologia. La modellazione delle minacce aiuta a trovare problematiche di progettazione anche prima della stesura del codice e questa fase risulta essere il momento migliore per scoprire tali problemi.

5.5.2.2 Comprensione dei requisiti di sicurezza

Individuare le minacce e decidere come s'intende procedere, rende chiari i requisiti. Con i requisiti più chiari, è possibile dedicare maggior energia a un insieme consistente di funzionalità e proprietà di sicurezza. Esiste un'importante interazione tra requisiti, minacce e mitigazioni. Durante la fase di modellazione delle minacce, è possibile scoprire ad esempio, che alcune minacce non sono conformi ai requisiti aziendali e come tali potrebbero non essere prese in considerazione. Altresì i requisiti di sicurezza potrebbero dover tener conto di ulteriori minacce la cui risoluzione potrebbe però, essere troppo complessa e dispendiosa, pertanto, si dovrà scegliere tra l'indirizzare parzialmente tali minacce o accettarle comunicando che non è possibile affrontarle.

5.5.2.3 Ingegnerizzazione e rilascio di prodotti più sicuri

Considerando i requisiti e la progettazione effettuati all'inizio del processo, è possibile ridurre drasticamente le probabilità di dover ri-progettare o ricostruire il sistema, o manutenere un flusso costante di bug di sicurezza. L'effort risparmiato in tal senso potrebbe andare a favore di un processo di costruzione di un prodotto migliore, più veloce, più economico o più sicuro, lasciando spazio a una maggiore concentrazione nella fase realizzativa dei requisiti funzionali.

5.5.3 Processo di modellazione del sistema da proteggere

Il processo di modellazione delle minacce s'identifica in un insieme di passi che realizzano dei sotto-obiettivi, piuttosto che come una singola attività. Essenzialmente, le domande da porsi al fine di identificare i sotto-obiettivi, sono:

- Cosa si sta realizzando?