- Identificazione delle minacce. Utilizzando la STRIDE o un albero delle minacce per facilitare l'enumerazione delle stesse.
    - STRIDE è un acronimo di spoofing, tampering, repudiation, information disclosure, denial of service e elevation of privilege. Queste descrizioni di vulnerabilità non sono intese come categorie che si escludono a vicenda, ma piuttosto come una tecnica euristica per l'enumerazione. Esaminare ciascun componente, ponendo particolare attenzione sui confini di fiducia, valutando se questo presenta vulnerabilità precedentemente indicate.
    - Gli Attack tree, possono eventualmente sostituire la STRIDE.
- Documentazione delle minacce.
- Valutazione delle minacce secondo il modello DREAD, un acronimo che indica il danno potenziale, la riproducibilità, l'utilizzabilità, gli utenti interessati, l'esposizione. Le minacce che si collocano ai primi posti in ciascuna di queste categorie dovrebbero avere una priorità più elevata nella risoluzione.

6.3 Modellazione e Individuazione delle minacce con STRIDE

Un evidente vantaggio dell'approccio STRIDE è l'indipendenza dal codice. Ciò è vantaggioso in quanto aiuta a identificare i problemi di sicurezza nella fase di analisi e progettazione del sistema software. Inoltre consente a tutto il team (oltre agli sviluppatori) di partecipare alla definizione del modello delle minacce del sistema stesso.
Il processo può portare benefici laddove non si dispone di un esperto di sicurezza all'interno del proprio team. L'impiego della STRIDE consente a questi team di individuare le vulnerabilità e le tecniche di mitigazione da attuare per difendersi dalle eventuali minacce identificate.
Le organizzazioni, possono inoltre beneficiare del processo sia per i nuovi progetti che per i progetti in essere, in cui potrebbero esistere delle vulnerabilità non identificate. L'implementazione di una metodologia che identifica e classifica le minacce è un processo ripetibile strutturato che può portare benefici a qualsiasi tipo di progetto.
Il risultato finale è, un elenco di vulnerabilità che i team di sviluppo e gli stakeholder dei prodotti possono quindi valutare, al fine di effettuare una accurata valutazione dei rischi, che insistono sulle vulnerabilità individuate.
La STRIDE è stata identificata come metodologia leader di Threat Modeling nell'industria del software.
Il successo di questa metodologia è dovuto ad un approccio ben strutturato alla modellazione delle minacce, ed è un eccellente supporto ed una risorsa per il team.
A volte la STRIDE viene indicata come "categorie STRIDE" o " tassonomia STRIDE". Tuttavia si evidenzia che la STRIDE non nasce come strumento di categorizzazione, ma con l'obiettivo di aiutare a trovare i possibili attacchi alla sicurezza.

6.4 Valutazione del rischio derivante dalle minacce individuate con DREAD

La metodologia DREAD è stata sviluppata da Microsoft nell'ambito della definizione del Security Development Lifecycle e del Threat Modeling. L'adozione della metodologia DREAD prodiga i seguenti benefici:

1. è utile per focalizzarsi sui reali rischi di una minaccia specifica;
2. obbliga a considerare fattori aziendali come la criticità del sistema e l'impatto sul business;
3. le cinque categorie sono tra loro scarsamente correlate (una di esse non implica le altre): considerare fattori indipendenti è un'ottima garanzia per formulare una corretta valutazione del rischio.