



X – possibile classe di minaccia per l'elemento indicato

* – applicabile solo se l'archivio dati contiene dati di logging o di auditing

Tabella 6 - STRIDE per elemento DFD

Le minacce STRIDE sono esattamente l'opposto di alcune delle proprietà che il nostro sistema dovrebbe avere, ovvero: autenticità, integrità, non ripudio, riservatezza, disponibilità e autorizzazione. La seguente tabella, mostra la correlazione tra la categoria di minacce STRIDE, la corrispettiva proprietà che si desidera mantenere, e gli elementi del sistema che sono tipicamente esposti alla classe di minacce indicata.

MINACCIA	PROPRIETA' VIOLATA (requisito o controllo di sicurezza)	TIPICA VITTIMA
Spoofing	Autenticazione	Processo Entità esterna Persona
Tampering	Integrità e Privacy (*)	Processo Archivio dati Flusso dati
Repudiation	Non ripudio/(Autenticazione+Integrità) (*)	Processo
Information Disclosure	Confidenzialità e Privacy (*)	Processo Archivio dati Flusso dati
Denial of Service	Disponibilità e Privacy (*)	Processo Archivio dati Flusso dati
Elevation of Privilege	Autorizzazione	Processo

Tabella 7 - STRIDE proprietà violate

(*) Articoli 25 e 32 del GDPR.

Ad esempio, alcuni elementi quali un flusso di dati tra due componenti, un processo o un archivio di dati; in base alla classificazione STRIDE sono potenzialmente vulnerabili a manomissioni, divulgazione di informazioni e negazione del servizio. Il processo di modellazione delle minacce prende in considerazione ogni minaccia per elemento e valuta se esistono tecniche di mitigazione adeguate per quel tipo di minaccia. Analizzando ciascun elemento del sistema come identificato nei DFD, viene creato un profilo di minaccia dell'applicazione.

La classificazione STRIDE contiene elementi orientati ai dati e alle transazioni. La sicurezza orientata ai dati è rappresentata dalla "triade CIA o RID" e delinea tre distinti principi di base che i sistemi sicuri dovrebbero seguire. Tali principi garantiscono la riservatezza, l'integrità e la disponibilità dei dati o delle comunicazioni. Le minacce STRIDE di divulgazione delle informazioni, manomissione e negazione del servizio sono direttamente correlabili alla triade CIA o RID. Segue una breve descrizione di queste tre tipologie di minaccia:

- Le minacce di divulgazione delle informazioni esistono nel momento in cui la parte malintenzionata può ottenere "un numero elevato di informazioni" in quanto il sistema non è in grado di far rispettare lo stato di confidenzialità delle informazioni stesse.
- Le minacce di manomissione si verificano quando il sistema è soggetto ad attacchi capaci di alterare i dati o le comunicazioni, invalidando così l'integrità dei dati a riposo o in transito.
- Il diniego del servizio è una minaccia alla sicurezza che riduce intenzionalmente la qualità del servizio, rendendolo non più performante, affidabile o disponibile.