6 LINEE GUIDA PER L'INDIVIDUAZIONE E LA RIVISITAZIONE DEI REQUISITI DI SICUREZZA E DI PRIVACY APPLICATIVI

6.1 Linee guida per la modellazione delle minacce

6.1.1 Identificazione degli obiettivi di sicurezza

La sicurezza dei dati è assicurata quando vengono garantite tre caratteristiche di fruizione di questi ultimi, che sono la riservatezza, l'integrità e la disponibilità.
Per raggiungere la sicurezza vengono eseguite azioni, che in caso di:

- riservatezza, proteggono i dati al fine di contrastare la divulgazione non autorizzata;
- integrità, contrastano le modifiche non autorizzate dei dati;
- disponibilità, contrastano la indisponibilità malevola dei dati/servizi.

Gli obiettivi specifici di sicurezza sono un sottoinsieme degli obiettivi di progetto e dovrebbero essere utilizzati per guidare gli sforzi impiegati nella modellazione delle minacce.
Identificare i principali obiettivi di sicurezza permette di concentrarsi con maggiore attenzione sulle aree da proteggere. Ad esempio, se si identificano i dettagli del profilo cliente come dati riservati, che devono essere protetti, è possibile esaminare la modalità di archiviazione sicura di tali dati e il modo in cui l'accesso a tali dati viene controllato e verificato.
Per determinare gli obiettivi di protezione, occorre porsi le seguenti domande:

- Quali dati occorre proteggere?
- Esistono requisiti di conformità? I requisiti di conformità possono includere criteri di protezione, leggi sulla privacy, regolamenti e standard.
- Esistono requisiti di qualità specifici del servizio? I requisiti di qualità del servizio includono tipicamente la disponibilità e i requisiti prestazionali.
- Esistono beni immateriali che devono essere protetti? Tali beni includono ad esempio, la reputazione dell'organizzazione, le informazioni commerciali sensibili e la proprietà intellettuale.

Di seguito sono riportati alcuni esempi di obiettivi di sicurezza comuni:

- Impedire agli aggressori di ottenere dati sensibili, inclusi i codici di accesso e le informazioni sul profilo.
- Soddisfare gli accordi a livello di servizio per la disponibilità delle applicazioni.
- Proteggere la credibilità dell'organizzazione.

6.1.2 Creazione di un disegno ad alto livello dell'applicazione

La modellazione delle minacce è un processo iterativo di analisi, dove ad ogni ciclo si scende sempre più in dettaglio, identificando di livello in livello le funzionalità chiave dell'applicazione, le sue caratteristiche ed i dati da proteggere.
Per avere una panoramica dell'applicazione occorre:

- Disegnare lo scenario di sviluppo dall'inizio alla fine;
- Identificare i ruoli;
- Identificare gli scenari d'uso più significativi;
- Identificare le tecnologie;
- Identificare i meccanismi di sicurezza.

Di seguito sono riportati i dettagli di ciascuna fase.
Disegnare lo scenario di sviluppo dall'inizio alla fine - La prima attività consiste in una modellazione ad alto livello dell'applicazione (composizione e struttura dell'applicazione, relativi sottosistemi e caratteristiche di distribuzione). Dopo il primo disegno, si aggiungono i dettagli sui meccanismi di autenticazione, autorizzazione e comunicazione. Da notare che quando si inizia la