Per ridurre la superficie d'attacco è necessario stabilire quali devono essere i privilegi minimi per ciascun componente dell'applicazione. Nella gestione della sicurezza delle risorse (quali Database, Active Directory, file, etc.), i ruoli applicativi devono essere quindi stabiliti a partire dalla logica di business con l'obiettivo di delimitare il perimetro di azione nell'accesso alla risorsa.

6.1.2.2 Identificare gli Scenari d'Uso Chiave

In questa fase occorre identificare le principali funzionalità e modalità d'uso e dettagliare gli aspetti legati alle attività di creazione, lettura, aggiornamento e cancellazione dei dati. Le caratteristiche chiave vengono spesso descritte nel contesto dei casi d'uso e consentendo la comprensione di come l'applicazione è destinata ad essere utilizzata e come può essere utilizzata in modo improprio. I casi d'uso permettono di identificare i flussi di dati e di focalizzarsi sull'analisi di eventuali minacce nelle fasi successive di dettaglio della modellizzazione.

6.1.2.3 Identificare le Tecnologie

Occorre identificare tutte le tecnologie utilizzate e le loro caratteristiche: Sistemi operativi; Server Web; Server di Base Dati; le tecnologie utilizzate per implementare la presentazione dei dati a livello utente, per gestire le regole di business, per l'accesso ai dati sottostanti e il linguaggio di sviluppo utilizzato.
L'identificazione delle tecnologie consente di concentrarsi sulle minacce che possono nascere in un momento successivo alla modellizzazione, legate alle specifiche tecnologie in uso. Inoltre, aiuta a determinare le eventuali tecniche di mitigazione del rischio.

6.1.2.4 Identificare Meccanismi di Sicurezza Applicativa

Un'altra fase importante è l'identificazione dei meccanismi di sicurezza applicativa, in particolare occorre analizzare i seguenti aspetti:

- Validazione input e dati;
- Autenticazione;
- Autorizzazione;
- Gestione della configurazione;
- Dati sensibili;
- Gestione della sessione;
- Crittografia;
- Manipolazione dei parametri;
- Gestione delle eccezioni;
- Audit e gestione dei log.

Lo scopo dell'identificazione di questi elementi è quello di aggiungere il più possibile ulteriori dettagli, anche poco conosciuti. Ad esempio è utile documentare come l'applicazione viene autenticata dalla base dati o come gli utenti vengono autorizzati, oppure quali sono le aree preposte all'autenticazione e all'autorizzazione.

6.1.3 Scomposizione dell'applicazione

La scomposizione dell'applicazione è utile per scoprire le minacce e le vulnerabilità del sistema. Nell'ottica di sicurezza, i componenti più importanti sono:

- confini di fiducia (trust boundaries);
- flussi di dati;
- punti di ingresso (entry points);
- punti di uscita (exit points).