7 UN ESEMPIO APPLICATIVO: CASO D'USO "EASY WEB SITE"

Lo use case si riferisce a un classico sito web disponibile su Internet che implementa un servizio per i propri clienti, i quali vi accedono attraverso un browser.
A titolo di esempio, si suppone che:

- il sito web acceda a una base dati di tipo SQL sia in lettura sia in scrittura;
- il sito web esponga funzionalità sia per i clienti del servizio sia per gli amministratori del servizio;
- l'utenza non autenticata (ad esempio, gli anonymous users) non possa accedere al sistema.

Sulla base delle assunzioni fatte, andiamo a rappresentare il sistema in oggetto attraverso un diagramma, facendo uso del simbolismo DFD, tipicamente utilizzato nella modellazione delle minacce (vedi paragrafo 5.5.3.1). Il diagramma che segue, mostra una scomposizione del sistema in oggetto ponendo in evidenza quelle che sono le sue componenti principali (Browser Client, Web Server e SQL Database), i confini di fiducia (Generic Trust Border Boundary e Internet Boundary) nonché i flussi dati di interscambio tra le singole componenti del sistema ([BC2WS] HTTPS Req (Credentials&Data) - Browser Client to Web Server, [WS2BC] HTTPS Req (Data) - Web Server to Browser Client, [WS2SQLDB] (Credentials&Data) Web Server to SQL Database e [WS2SQLDB] (Data) SQL Database to Web Server) dette anche interazioni.

7.1 Diagramma: Use Case

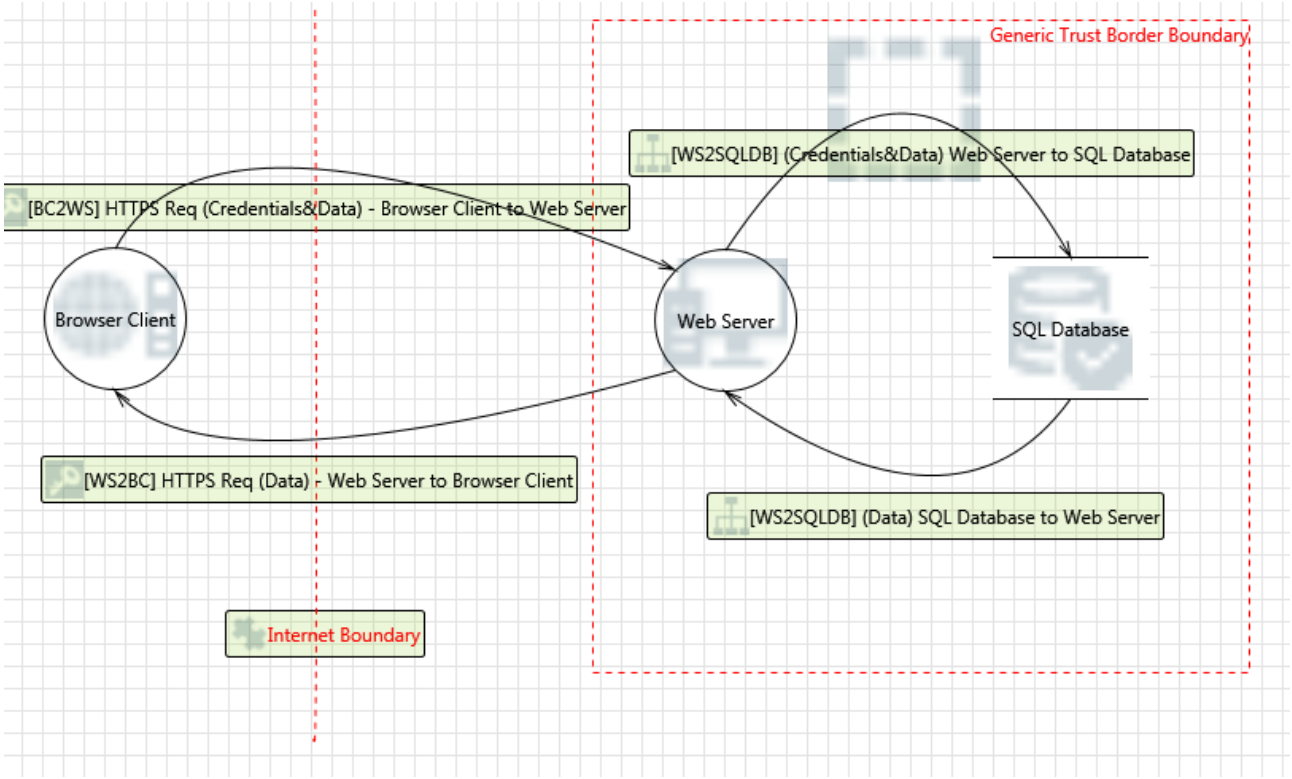

Figura 9 - Diagramma dello use case

A seguire, per ciascuna interazione/flusso dati, vengono individuate le possibili minacce sulla base dell'analisi STRIDE. Per ciascuna minaccia viene fornita la categoria STRIDE/Compliance di pertinenza a cui la minaccia appartiene, una breve descrizione e alcune contromisure da attuare nel processo di mitigazione. Viene inoltre indicato, attraverso l'analisi DREAD, un indice di priorità (ALTO, MEDIO e BASSO) da considerare nella risoluzione della minaccia stessa (DREAD Score).