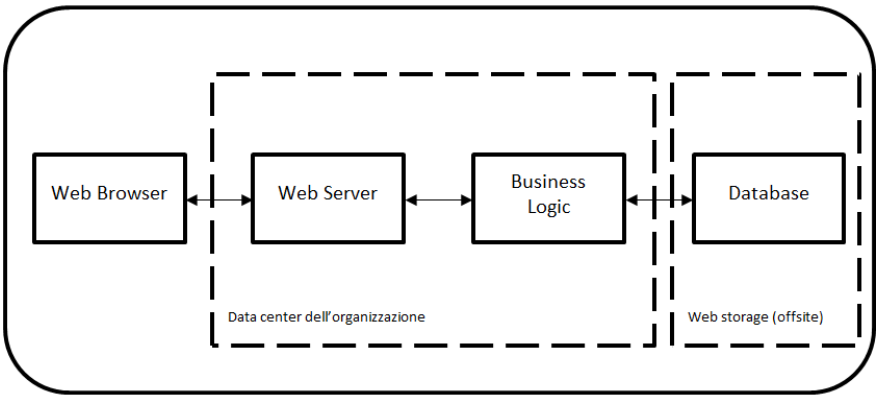

Figura 6 - Aggiunta dei "Trust boundaries" al diagramma

Quando il diagramma diventa più grande e più complesso, può essere molto utile numerare ogni processo, flusso dati e archivio dati presenti nel diagramma, come mostra la figura che segue (Ciascun "trust boundary" dovrebbe avere un identificativo univoco in rappresentanza del suo contenuto):

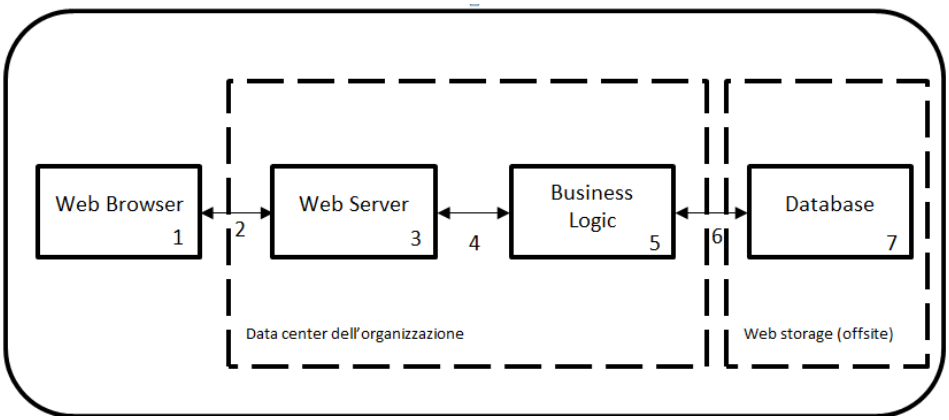

Figura 7 - Numerazione degli elementi del diagramma

Si deve pensare al diagramma del modello come parte integrante del processo di sviluppo, quindi deve essere messo sotto il controllo di versionamento così come tutto il resto del materiale relativo al progetto. Da questo modello, si procede con l'individuazione delle minacce sulla base delle metodologie e delle tecniche descritte nel paragrafo successivo.

5.5.4 Tecniche di modellazione e individuazione delle minacce

L'obiettivo che tutte le metodologie di modellazione delle minacce condividono è lo sviluppo di un processo di passi iterativi che un team può facilmente seguire durante la valutazione di un sistema software.

5.5.4.1 Microsoft SDL – STRIDE

La STRIDE è un processo metodologico che aiuta a individuare le minacce di sicurezza in un sistema complesso. L'elemento mnemonico STRIDE è acronimo di Spoofing, Tampering, Repudiation, Information disclosure, Denial of service ed Elevation of privilege.
Si riporta a seguire la descrizione delle classi di minaccia rappresentate dalla STRIDE:

- **Spoofing** (falsificazione di identità): è la pretesa di essere qualcos'altro o qualcun altro che non si è. Classifica l'insieme delle minacce che consentono a un attaccante di interagire con il sistema