Entrambi si basano sul parere del singolo individuo/team che effettua la valutazione del rischio. La DREAD ha perfezionato il suo sistema di valutazione del punteggio riducendo la probabilità di variazione dei risultati ed offre un approccio strutturato che i team possono adottare. Il processo è inoltre ben documentato e relativamente facile da attuare. Questa è una delle possibili motivazioni per cui scegliere l'analisi DREAD rispetto a S. B. S. R. S.

5.7.3 Altri processi di valutazione del rischio

Esistono altre opzioni disponibili per la valutazione del rischio, come l'US-CERT Vulnerability Metric, che utilizza una metrica quantitativa e valuta la gravità di una vulnerabilità assegnandole un valore compreso tra 0 e 180. Il Common Vulnerability Scoring System (CVSS) mira a fornire un framework open per misurare l'impatto delle vulnerabilità IT, mentre la scala SANS Critical Vulnerability Analysis classifica le vulnerabilità utilizzando diversi fattori chiave e variando il grado di peso. Il processo di valutazione del rischio da adottare dipende essenzialmente dalla scelta individuale del team che realizza il Threat Model.

5.8 Privacy by Design

5.8.1 Introduzione e concetti base

Il regolamento generale sulla protezione dei dati personali (UE) n. 679/2016 ("GDPR") è entrato in vigore, a partire dal 25 maggio 2018, come principale quadro giuridico in materia di protezione dei dati nell'UE direttamente applicabile in tutti gli Stati membri, abrogando la direttiva 95/46/CE sulla protezione dei dati. In particolare, in Italia, il decreto legislativo n. 101/2018 adegua la normativa nazionale al nuovo Regolamento, con l'entrata in vigore del 19 settembre 2018. Il regolamento prevede un'armonizzazione del regime giuridico di protezione dei dati in tutta l'UE, rafforzando i diversi principi e obblighi della direttiva che abroga e introduce nuove disposizioni quali la protezione dei dati per default e a partire dalla progettazione. Al fine di migliorare la trasparenza delle operazioni di trattamento da parte dei responsabili del trattamento e degli incaricati del trattamento, il regolamento introduce, inoltre, disposizioni specifiche in materia di certificazione, sigilli e marchi.
La garanzia di sicurezza di un'organizzazione rappresenta la base per la protezione della privacy degli individui. La privacy può essere compromessa a causa di un errore nella sicurezza, tuttavia, la privacy si riferisce all'utilizzo improprio e non, delle informazioni da parte di utenti autorizzati. La privacy è una politica di gestione delle informazioni più che una politica di controllo accesso. Insieme, privacy e sicurezza, rappresentano la base per creare un solido rapporto di fiducia. Una sicurezza solida è la base della protezione della privacy. La privacy richiede una sicurezza effettiva, ma quest'ultima da sola, non garantisce una privacy effettiva. La sicurezza garantisce ad esempio il controllo accessi alle risorse di un'organizzazione attraverso un'istruzione di controllo accessi come: all'entità X è consentito eseguire l'operazione Y sulla risorsa Z che tradotta in un esempio pratico, potrebbe essere: "Il personale del settore finanziario può interrogare la base dati della contabilità". La privacy si riferisce alla relazione tra un'organizzazione che raccoglie informazioni e il proprietario delle informazioni raccolte. Per stabilire e gestire questa relazione, è necessario creare una politica di riservatezza formata da diverse istruzioni. Un'istruzione della politica di riservatezza definisce:

- I tipi di informazioni raccolte e quelle accessibili;
- Chi può accedere alle informazioni raccolte;
- Per quali scopi è possibile accedere a tali informazioni.

Suddetta istruzione può assumere la seguente forma: all'entità X è consentito eseguire l'operazione Y sulla risorsa protetta Z del proprietario A per lo scopo B solo se il proprietario A esprime il proprio consenso esplicito. Una possibile traduzione di tale concetto in un esempio pratico,