rischio direttamente all'utente utilizzatore, chiedendogli di navigare attraverso una moltitudine di finestre di dialogo incomprensibili prima che questo possa effettivamente utilizzare il sistema. Ovviamente questa non vuole essere assolutamente una tra le migliori soluzioni, ma in alcuni casi esiste da parte degli utilizzatori una conoscenza tale da poterli rendere partecipi per convenire ad un giusto compromesso di sicurezza. Se si pensa che esistano i presupposti per una soluzione del genere, si dovrebbe sostenere chi usa il sistema a prendere una decisione in tal senso.

- **Accettare** la minaccia - È l'ultimo approccio per indirizzare una minaccia. In alcuni casi, il costo necessario per impedire a qualcuno di inserire una back-door nella scheda madre di un hardware aziendale potrebbe risultare elevato, quindi in tal caso si potrebbe scegliere di accettare il rischio. Una volta che questo viene accettato, non c'è più bisogno di preoccuparsene. A volte la preoccupazione indica che il rischio non è stato pienamente accettato o che l'accettazione del rischio non sia appropriata.

5.7 Valutazione del rischio: tecniche di Risk Ranking

5.7.1 DREAD

Microsoft ha sviluppato la metodologia DREAD (tabella che segue) per valutare ciascun rischio individuato durante l'attività STRIDE. Ad ogni rischio viene assegnato un punteggio DREAD da parte del team di sicurezza/sviluppo i quali realizzano e applicano il modello delle minacce.
Esistono diverse varianti del sistema di valutazione e prioritizzazione del rischio:

DREAD	DESCRIZIONE
Damage potential	Classifica l'estensione del danno che si verifica se viene sfruttata la vulnerabilità individuata.
Reproducibility	Classifica quanto spesso un tentativo di sfruttamento della vulnerabilità individuata viene portato a termine con successo.
Exploitability	Assegna un valore numerico allo sforzo necessario per sfruttare la vulnerabilità individuata. Inoltre, la possibilità di sfruttamento considera come condizioni preliminari che l'utente deve essere autenticato.
Affected Users	Assegna un valore numerico che rappresenta la numerosità degli utenti del sistema che potrebbero essere interessati se un exploit divenisse ampiamente disponibile.
Discoverability	Misura la probabilità che la vulnerabilità possa essere individuata da soggetti esterni della sicurezza e/o dagli hacker, se questa non viene risolta tramite patch.

Tabella 21 - Modello DREAD

Nella valutazione del rischio ad ogni componente DREAD viene assegnato un punteggio. I punteggi dei singoli componenti vengono quindi calcolati per dare un 'punteggio DREAD' totale.
Il rischio viene quindi determinato in base al valore che il punteggio "DREAD" assume rispetto ad intervalli di valori predefiniti. Il risultato finale è un elenco di vulnerabilità classificate per rischio.
Il processo di applicazione della metodologia DREAD è estremamente soggettivo e richiede le necessarie competenze. È consigliabile avere almeno un membro del team che abbia competenze sulla sicurezza per dare il necessario supporto nell'assegnazione dei punteggi DREAD.
Come fase finale del processo di modellazione delle minacce, viene attuata una valutazione del ***rischio***[34], per dare una priorità a ciascuna vulnerabilità indentificata.

[34] Da non confondersi con l'attività di Risk Assessment per la quale si deve far riferimento alla metodologia e al tool sviluppato da AGID a tale scopo (**Cyber Risk Management** - **https://www.sicurezzait.gov.it/Home**). Per ulteriori dettagli si rinvia all' *Allegato 1- Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro*.