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*.

In generale, in termini quantitativi, il rischio è definito come il prodotto tra la probabilità di accadimento dell'evento e l'impatto:

Rischio = Probabilità x Impatto

In effetti, se almeno uno dei due termini del prodotto tende a zero, percepiamo il rischio come basso. Viceversa percepiamo un rischio grave quando ambedue i termini sono elevati.
Nella metodologia DREAD il concetto di "impatto" viene declinato in termini di:

1. danno (Damage)
2. utenti interessati (Affected Users)

mentre il concetto di "probabilità" viene declinato in termini di:

3. riproducibilità (Reproducibility),
4. sfruttabilità (Exploitability)
5. rilevabilità (Discoverability).

DREAD è appunto l'acronimo che "fattorizza" il rischio rispetto a queste 5 distinte categorie che caratterizzano la minaccia:

1. **Damage potential**: Quanto sarebbe rilevante il danno nel caso in cui la minaccia[35] si concretizzasse?
2. **Reproducibility**: Quanto è facile che la minaccia possa ripetersi?
3. **Exploitability**: Quanto tempo, sforzo e conoscenza sono necessarie per concretizzare con successo la minaccia?
4. **Affected Users**: Nel caso in cui la minaccia si concretizzi, quale percentuale di utenti sarebbe coinvolta?
5. **Discoverability**: Quanto è facile per un attaccante scoprire la possibilità di minaccia?

A ciascuna categoria viene attribuito un peso. Il "DREAD score" è la media dei 5 pesi, ossia:

DREAD Score= (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5

Occorre quindi valutare e dare un peso numerico alle cinque categorie della tabella sopra mostrata. A seconda del dominio considerato, ci si può riferire o a una scala (semplificata) di tre soli valori o a una scala (più granulare) a dieci valori. I valori crescono rispettivamente al crescere del danno, della facilità di riproduzione, della facilità di sfruttamento, del numero di utenze coinvolte, della facilità di rilevamento.
A titolo di esempio, si consideri la categoria "Exploitability":

- nel caso si voglia adottare una scala a 3 valori si potrebbero voler considerare e pesare in modo diverso i seguenti casi (Quanto è difficile sfruttare la vulnerabilità?):
    - 1= L'attacco richiede una figura senior e una conoscenza profonda del sistema attaccato; un'utenza con diritti di amministrazione; dispendio di parecchie risorse per organizzare l'attacco (es. impiego di custom tool);
    - 2 = L'attacco richiede una figura senior; un'utenza autenticata con abilità non amministrative; tool di attacco disponibili in rete;
    - 3 = L'attacco è alla portata di una figura junior; senza necessità di autenticazione; attraverso un web browser.

35 Si ricordi che la minaccia è un evento potenziale, accidentale o deliberato. Se deliberato, la minaccia si configura come attacco.