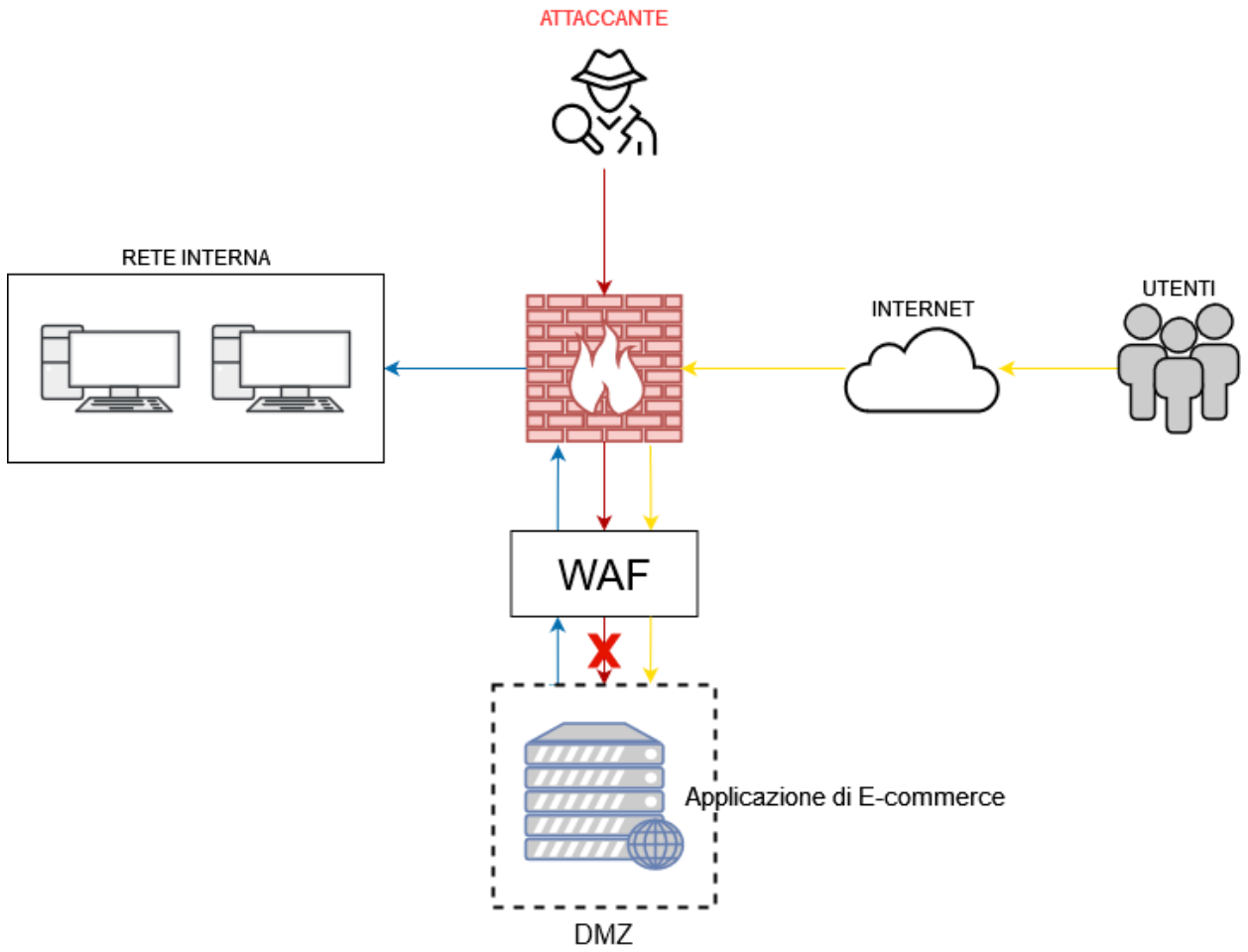
In questo esercizio andremo a prevenire attacchi tipo SQLi e XSS alla web app, valutare il danno economico a fronte di un attacco DDoS ed infine, tramite un incident response plan cercare di arginare o annullare i danni alla rete interna.

Partendo dalle **azioni preventive**; abbiamo installato un WAF come in figura, tra la DMZ ed il firewall, per prevenire al meglio eventuali azioni sospette o malevole da parte di un ipotetico attaccante.
In termini semplici, il WAF controllerà e filtrerà il traffico diretto alla web app, bloccando i contenuti ritenuti malevoli o sospetti.



Altre azioni preventive possono essere:
-**Il controllo dell'input utente**, visto che stiamo avendo a che fare con attacchi di tipo SQLi o XSS, ciò potrebbe rivelarsi fondamentale per prevenire questo tipo di attacchi ed evitare (nel caso del SQLi) l'iniezione di codice malevolo.

-**Formazione del personale**, utile in qualsiasi situazione per poter ridurre al minimo possibile il rischio di un errore umano.

-**Monitoraggio costante della rete**, per individuare prontamente ed agire di conseguenza nel caso in cui un attacco stia prendendo luogo.

Nel caso di un ipotetico attacco DDoS (Distributed Denial of Service), si ipotizza che il servizio diventi irraggiungibile ai clienti per circa 10 minuti. Gli utenti spendono in media circa 1.500€ ogni minuto, sulla piattaforma.
Con un semplice calcolo possiamo valutare una perdita di circa 15.000€ a fronte di un'interruzione di 10 minuti.

Questa perdita potrebbe essere ridotta o evitata con un corretto **BCP** (**Business Continuity Plan**, piano di continuità operativa), che permetterebbe ad un servizio di continuare ad operare anche in situazioni critiche, tipo un attacco DDoS, danni accidentali o addirittura calamità naturali.
Un **BCP** valido si baserebbe sull'identificare e pianificare i fattori di rischio, partendo da quelli più critici ed importanti (**Risk Assessment**), valutando l'impatto che questi avrebbero sull'azienda (**BIA, Business Impact Analysis**), formando il personale correttamente al fine di attuare il piano nel modo più efficiente e rapido possibile (per mantenere il servizio attivo al meglio delle possibilità), avendo a disposizione dei backup (possono essere strutture secondarie, sostituzioni di infrastrutture IT e via dicendo) ed infine migliorandolo e adattandolo costantemente per far fronte ai cambiamenti costanti, sia dentro, che fuori l'azienda.

Oltre al **BCP**, andrebbe sviluppato un **IRP (Incident Response Plan).** Al contrario del **BCP**, l'**IRP** serve uno scopo diverso. Ovvero il ridurre i danni causati da incidenti di sicurezza (come ad esempio una fuga di dati, o un'intrusione da parte di malintenzionati o un attacco informatico). Un **IRP** comprende alla fine le fasi di "**contenimento, eliminazione e recupero**":
- Contenimento e riduzione dei danni causati dall'incidente
- Eliminazione dell'incidente dai sistemi e dalle reti interessati
- Recupero dei servizi e dell'operatività di essi

Andremo a vedere nella prossima slide la prima di queste tre fasi in maniera pratica, ipotizzando una situazione realistica.

Come si può notare nell'immagine a destra, abbiamo applicato una misura di contenimento, in questo preciso caso, una rimozione completa della rete interna, per evitare ulteriormente la propagazione del malware. Pertanto la rete interna non ha accesso ad internet.

Questa è la misura più drastica possibile tra quelle di contenimento, ma è quella necessaria qualora bisogna prioritizzare l'integrità delle macchine critiche ed importanti.

Si può notare tra l'altro che così facendo l'attaccante mantiene l'accesso sulla DMZ, lasciando in balia del malware gli utenti dell'e-commerce. Evidentemente in questo caso l'azienda avrebbe valutato l'impatto di questo attacco e concluso che, a livello economico, sarebbe meglio "sacrificare" l'immagine (un'azienda che lascia in balia di un malware i propri utenti non è moralmente corretto) a favore di un danno economico-aziendale meno pronunciato. Ad esempio, l'azienda avrebbe potuto chiudere i battenti qualora il malware avesse infettato dei dispositivi di importanza critica e non ci fosse stato un backup valido per ripristinare i danni.