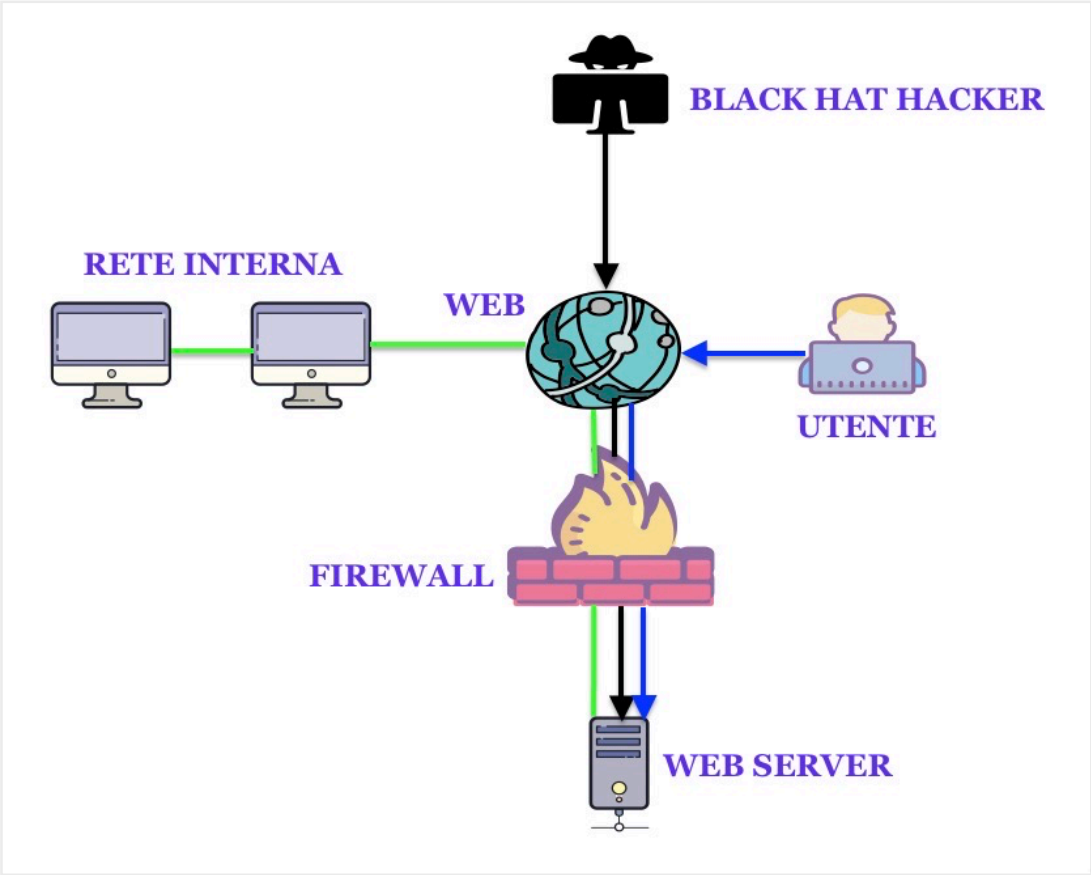
AZIONI PREVENTIVE -IMPATTI SUL BUSINESS-RESPONSE

TRACCIA:

L'ESERCIZIO DI OGGI PREVEDE DI SIMULARE AZIONI PREVENTIVE, CALCOLARE CHE IMPATTI ECONOMICI PUÒ AVERE UN'AZIENDA E RESPONSE IN CASO DI ATTACCO, IN MODO DA POTER FAR FRONTE AN UN IPOTETICO INCIDENTE E LIMITARE DANNI A ESSO CORRELATI.

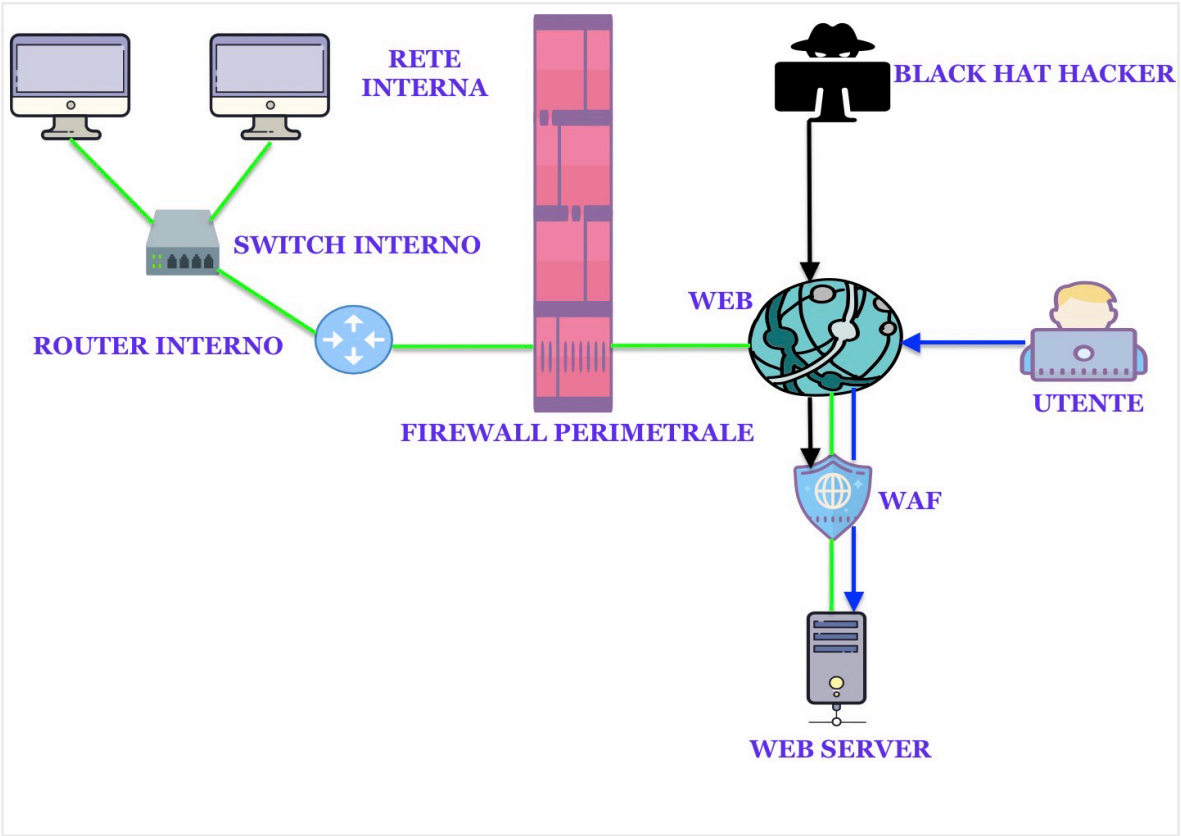
PRENDIAMO COME RIFERIMENTO QUESTA IMMAGINE:



Come possiamo notare in questo caso un utente con intenzioni malevoli, sfruttando una vulnerabilità contenuta nel firewall è capace di penetrale le sue difese e fare irruzione nella rete interna aziendale.

Per poter porre rimedio a questa situazione dobbiamo per prima cosa mettere al sicuro la rete interna attraverso un firewall perimetrale ed un router il quale andrà a filtrare ogni pacchetto sia in entrata che in uscita.

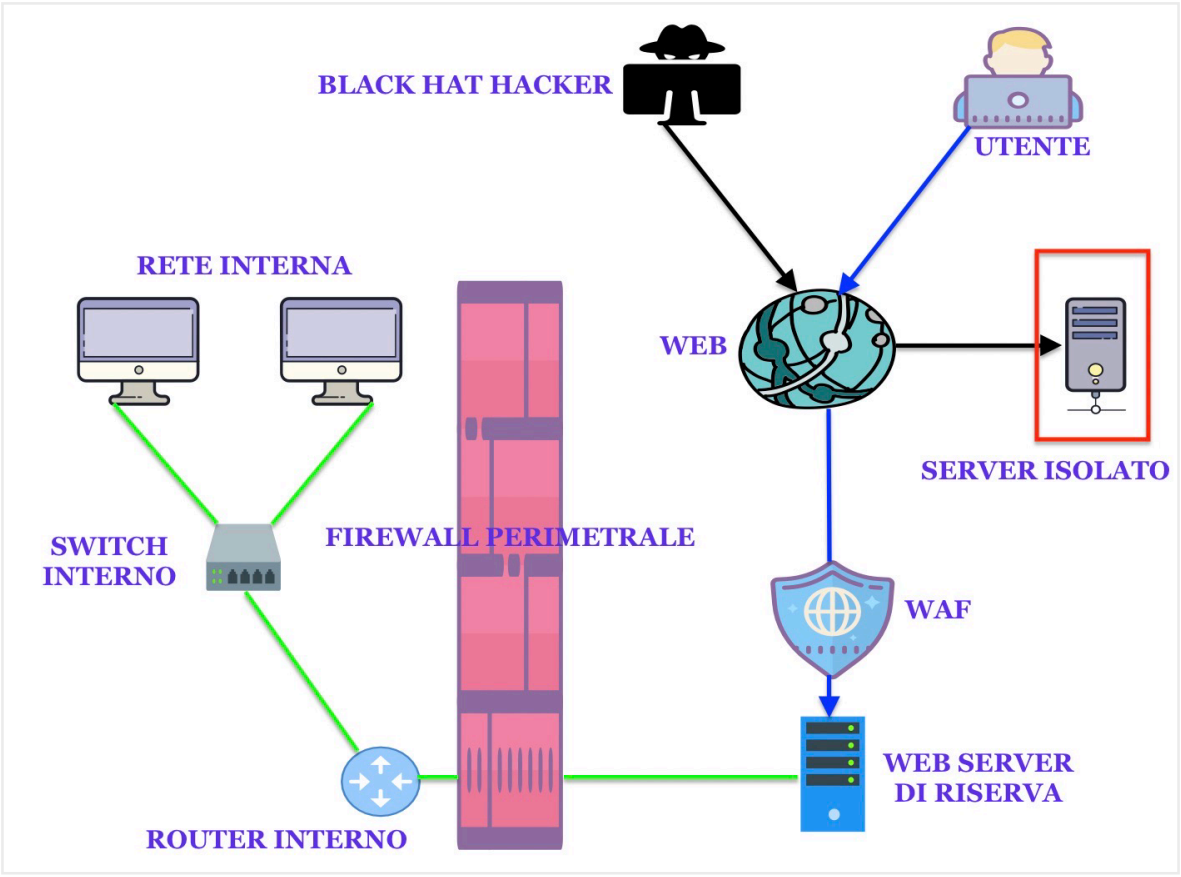
Per quanto riguarda il web server siamo andati ad applicare un WAF (Web Application Firewall) il quale settato con le giuste regole correttamente consente si di accedere alla pagina web, con l'unica differenza che va filtrare, ed aventualemente a bloccare eventuali azioni malevole registrandole nei log waf.



Questa immagine ci illustra una situazione più o meno simile alla precendente con l'unica differenza, che il malintenzionato è riuscito a penetrare le difese del web server.

in questo caso l'azienda ha deciso di applicare un approccio diverso ovvero il server infetto non è stato disattivato, ma solo isolato in modo da far credere al malintenzionato di avere il controllo della compagnia.

Nel frattempo ha messo in moto un server di riserva il quale prenderà il posto del server infetto indirizzando tutte le richieste provenienti dai vari utenti, in modo da non dover arrestare il sistema di rete.

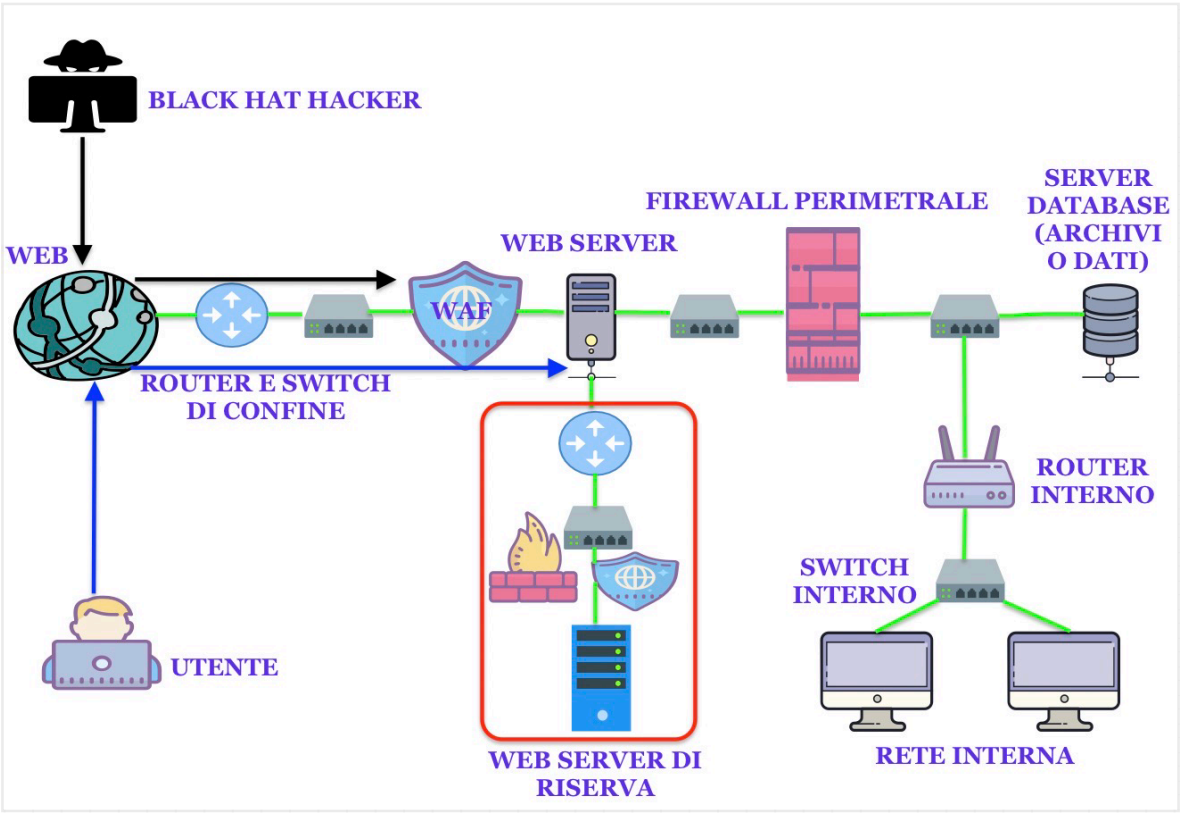


Infatti se questa contro misura se non sarebbe mai stata preventivata, la compagnia avrebbe potuto perdere ben 1500€ per ogni minuto che il server fosse stato inattivo.

Se ipotizziamo che la compagnia avesse ricevuto un attacco di tipo di DDoS, ci vogliono più o meno 10 minuti prima che l'applicazione torni a funzionare.

In termini economici quanto avrebbe impattato sull'azienda? Vediamolo insieme:
Se per ogni minuto di inattività dell'E-Commerce l'azienda perde 1500€, moltiplicato per 10 (che sono minuti che ci vogliono per ottenere risposta dall'applicazione), abbiamo come risultato un perdita di ben 15.000€ ogni dieci minuti.

Adesso capiamo bene il perché certe situazioni devono essere preventivate prima che accadano onde evitare ingenti perdite economiche.



Come ultima ma non per importanza ho riportato uno schema di difesa complesso, il quale garantisce a tutti gli utenti l'accesso al web però con specifiche regole ne blocca l'accesso alla rete interna.

Come se non bastasse qualora il malintenzionato dovesse bucare le difese, vi è un ulteriore server di riserva in grado di prendere il controllo della situazione in caso di crash di sistema, il quale è praticamente isolato ed inaccessibile sino a quando non vi sia la necessità di attivarlo.

Oltre a questo la rete interna è ben protetta da un firewall perimetrale regolato in modo da non consentire l'accesso a nessun utente al di fuori della propria rete aziendale, con tanto di server database in caso di perdita di dati da eventuali server esterni.