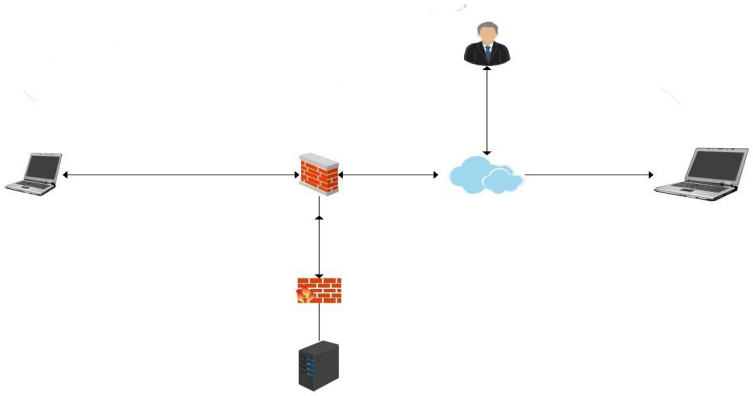
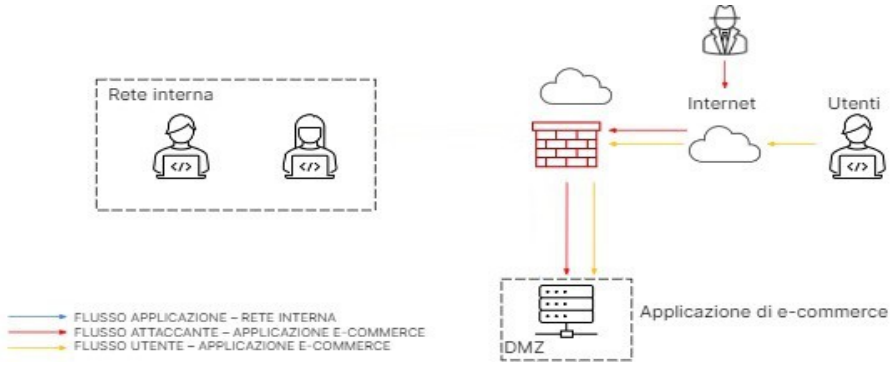
Progetto 5

1) L'azione preventiva che si può usare per evitare attacchi SQLi e XSS e aggiungere un WAF(Web Application Firewall) per evitare che il malintenzionato riesca ad attaccare tramite Web.

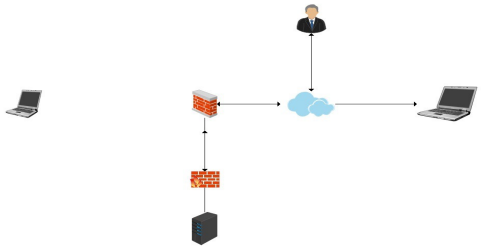


2) Subendo un attacco di tipo DDos che cessa l'attività del sistema per 10 minuti il danno economico è di 15.000€. L'azione preventiva che in questo caso si utilizza è di ridondanza, creando un backup dell'Aplicazione Web in modo tale che se viene attacato il sistema non cessa l'attività.

3) Avendo l' Applicazione Web attaccata da un hacker, la soluzione di response da attuare in questo caso è di isolamento, togliendo il flusso di dati che va dall'Applicazione Web alla rete interna così da limitare l'attaccante e no recare danni alla rete interna.



4) A



5)

Un metodo più aggressivo che si può implementare è la ridondanza del server dell'Applicazione Web aggiungendone uno uguale preceduto sempre dal WAF così in caso di malfunzionamento o attacco non si perde l'attività del sistema.

Si può aggiungere anche un IPS prima della rete interna, in modo da avere un controllo maggiore sui log, e in più se si dovesse ricevere un' attacco viene usato come azione preventiva, analizzando il flusso della rete rivelando in caso di attacco le attività anomale.