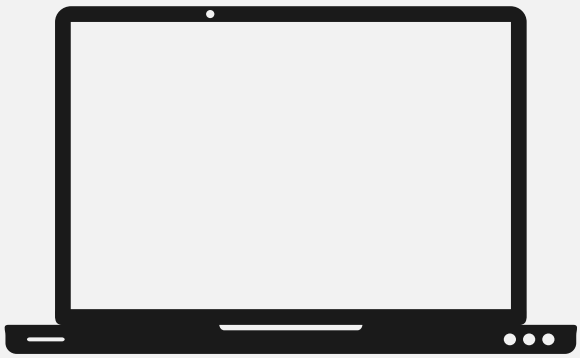


RELAZIONE S9L5

ANALISI SICUREZZA

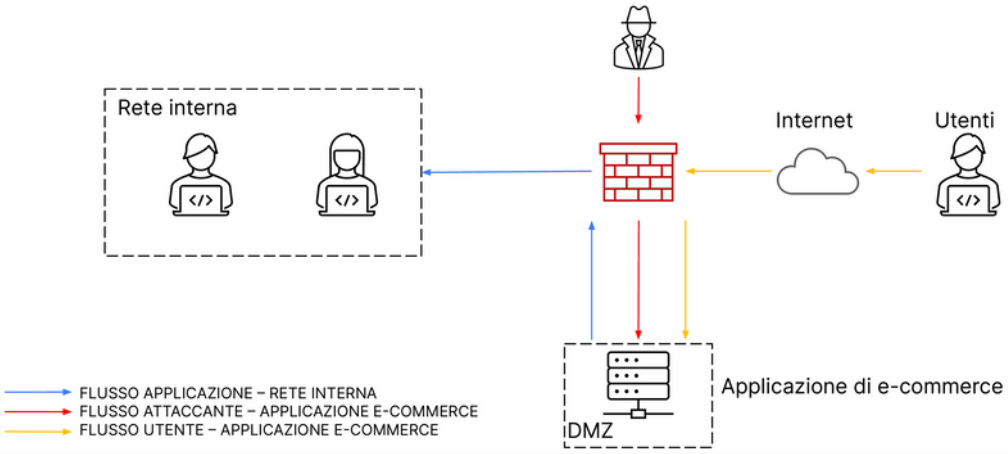
DAVIDE LECCI

corso cybersecurity 2023

ARCHITETTURA DELLA RETE

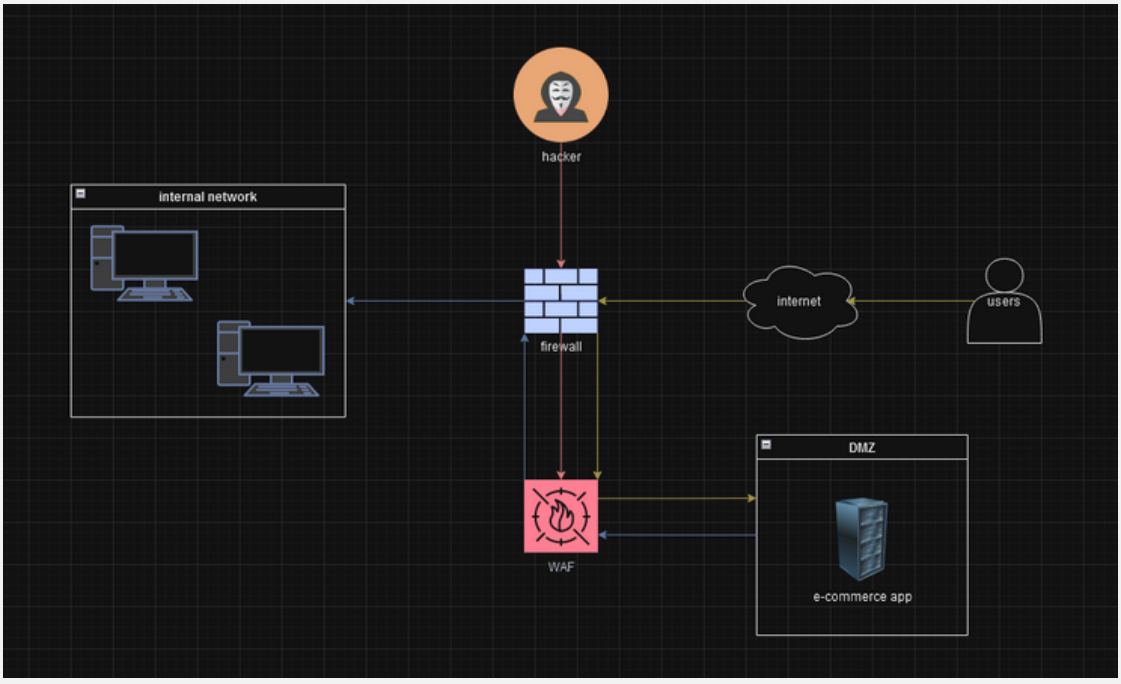
Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE: QUALI AZIONI PREVENTIVE SI POTREBBERO IMPLEMENTARE PER DIFENDERE L'APPLICAZIONE WEB DA ATTACCHI DI TIPO SQLI OPPURE XSS DA PARTE DI UN UTENTE MALINTENZIONATO? MODIFICATE LA FIGURA IN MODO DA EVIDENZIARE LE IMPLEMENTAZIONI

Tra le azioni preventive che possiamo attuare possiamo ricorrere all'uso di un **waf** per proteggere il web server. Quest'azione tuttavia andrebbe accompagnata da altri accorgimenti per aumentare il grado di protezione contro questi attacchi.
E' necessario sanificare gli input dell'applicazione per far si che accettino solo i valori che si aspettano impostando corrette regole di validazione. Sarebbe inoltre opportuno iniziare (se non già fatto) un'attività di monitoring del traffico sulla rete così da essere pronti nel caso si verifichino altri tipi di attacchi.
Qui di seguito è possibile vedere un'immagine con l'implementazione del waf:

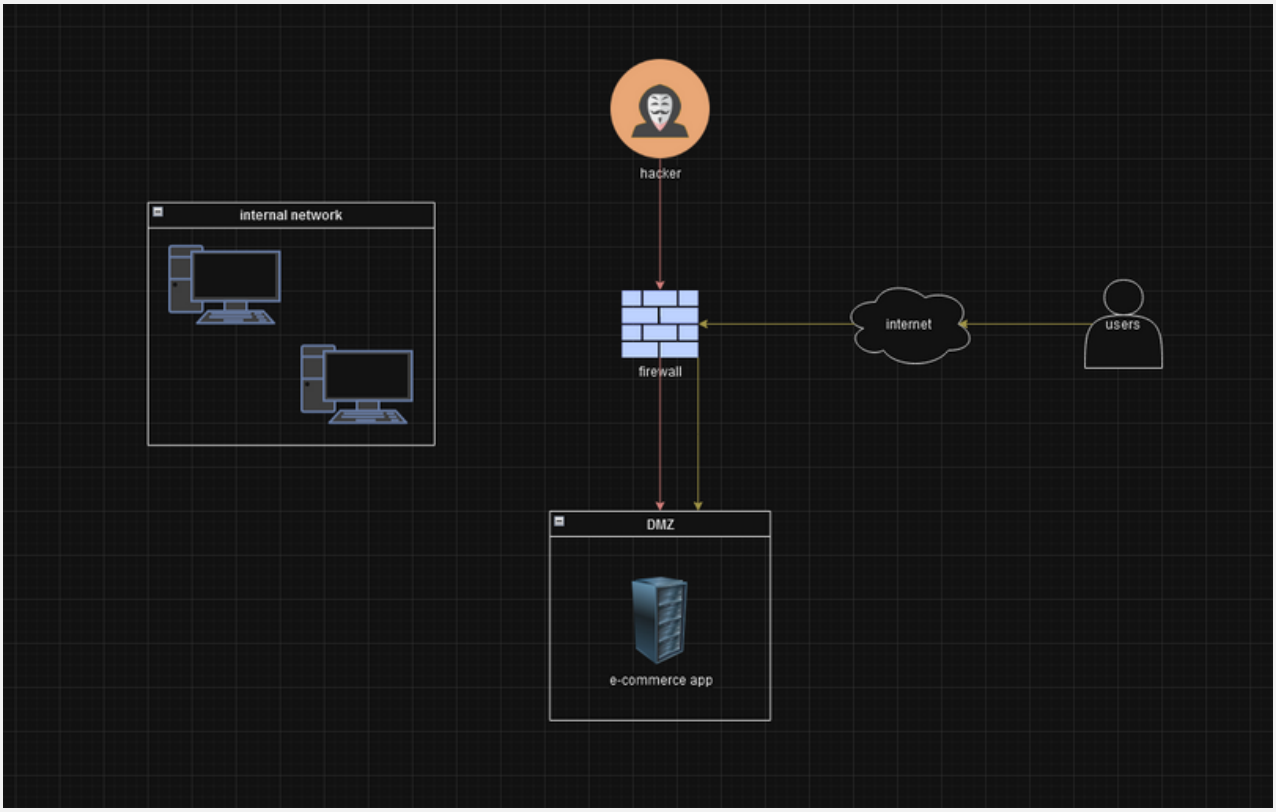


IMPATTI SUL BUSINESS: L'APPLICAZIONE WEB SUBISCE UN ATTACCO DI TIPO DDOS DALL'ESTERNO CHE RENDE L'APPLICAZIONE NON RAGGIUNGIBILE PER 10 MINUTI. CALCOLARE L'IMPATTO SUL BUSINESS DOVUTO ALLA NON RAGGIUNGIBILITÀ DEL SERVIZIO, CONSIDERANDO CHE IN MEDIA OGNI MINUTO GLI UTENTI SPENDONO 1.500 € SULLA PIATTAFORMA DI E-COMMERCE.

Se consideriamo che ogni minuto l'azienda guadagna 1.500€ allora per 10 minuti di irraggiungibilità l'azienda perderà 15.00 €. Tuttavia per dare ulteriori informazioni circa la gravità dell'impatto mancano dei dati a nostra disposizione come il fatturato mensile.
Presumilbilmente l'azienda non guadagnerà 1.500€ ogni minuto per 24 ore ma il guadagno varierà a seconda dei momenti della giornata nonché ai giorni della settimana. Non sappiamo neanche se questo guadagno sia dovuto ad una particolare offerta valida in un determinato periodo e quindi magari è un gadagno più alto del solito.
In mancanza di tutte queste variabili è impossibile dire se questo attacco avrà un impatto grave o meno.

RESPONSE: L'APPLICAZIONE WEB VIENE INFETTATA DA UN MALWARE. LA VOSTRA PRIORITÀ È CHE IL MALWARE NON SI PROPAGHI SULLA VOSTRE RETE, MENTRE NON SIETE INTERESSATI A RIMUOVERE L'ACCESSO DA PARTE DELL'ATTACCANTE ALLA MACCHINA INFETTATA. MODIFICATE LA FIGURA IN SLIDE 2 CON LA SOLUZIONE PROPOSTA.

Se non dobbiamo rimuovere l'applicazione web da internet allora si parla di **isolamento**, ovvero separeremo l'applicazione web dal resto dell'azienda in modo tale che il malware non possa propagarsi al suo interno.
Si può vedere la nuova struttura nella figura sottostante



Isolando così la rete interna il personale competente potrà provvedere a rimuovere il malware dall'ecommerce senza il pericolo che questo infetti la rete aziendale.
C'è da notare come comunque che le persone continueranno ad avere accesso all'ecommerce infetto e potenzialmente il malware potrà propagarsi molto velocemente. L'ideale sarebbe rimuovere l'ecommerce come per la rete interna così da non infettare ulteriori persone.
Potremmo utilizzare un'analisi quantitativa e calcolare il maximum tolerable downtime (MTD) e il recovery object time (RTO) per vedere se il tempo necessario per il recupero dell'asset è minore dell'MTD, in questo modo sapremo se l'azienda subirebbe perdite economiche irreparabili.
Un'altra soluzione potrebbe essere quella di istituire un'altra DMZ completamente separata con una copia del sito che venga aggiornata regolarmente, in caso di incidenti di sicurezza si potrebbe mettere online l'altro server. Questa operazione però ha come svantaggio i costi di mantenimento alti e un disallineamento tra i due server con conseguente impatto sull'ecommerce e molto probabilmente sulle vendite.