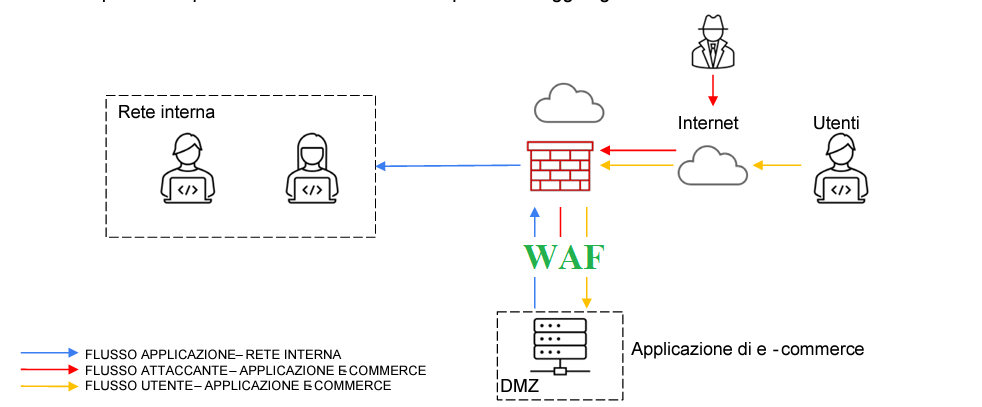
**Traccia:**

Con riferimento alla figura, rispondere ai seguenti quesiti.

1. 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;
2. 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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica;
3. Response: l’applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra 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;
4. Soluzione completa: unire i disegni dell’azione preventiva e della response (unire soluzione 1 e 3);
5. Modifica più aggressiva dell’infrastruttura, integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).
6. Per *azioni preventive* facciamo riferimento a tutte quelle misure, procedure o pratiche adottate per ridurre la probabilità di un evento dannoso o indesiderato nel contesto dell'utilizzo dei sistemi informatici. Queste azioni sono fondamentali per mitigare rischi e proteggere l'integrità, la riservatezza e la disponibilità delle risorse informatiche. Le azioni preventive sono un aspetto cruciale della sicurezza informatica e vengono spesso implementate insieme ad altre misure, come azioni correttive e di rilevamento, per fornire una difesa completa contro minacce e vulnerabilità.

In particolare, in questo caso è sicuramente necessario un **Web Application Firewall** **(WAF)** per proteggere le applicazioni da attacchi quali SQL injection e Cross Site Scripting (XSS). Un Web Application Firewall è un'applicazione o un servizio di sicurezza progettato per proteggere le applicazioni web da attacchi malevoli o indesiderati. Funziona come uno strato di protezione tra l'applicazione web e il traffico Internet, filtrando e monitorando il traffico HTTP/HTTPS in ingresso e in uscita per identificare e bloccare attacchi mirati alle applicazioni web.

****

1. Per calcolare l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco **DDoS**, possiamo utilizzare la seguente formula:

**Impatto finanziario = (Fatturato medio per minuto) \* (Numero di minuti di indisponibilità)**

Dato che gli utenti spendono in media 1.500 € sulla piattaforma di e-commerce ogni minuto, possiamo calcolare l'impatto finanziario come segue:

**1.500 €/min \* 10 min = 15.000 €**

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti costa all’azienda 15.000 €.

Nella valutazione di possibili azioni preventive da tale tipo di attacco, un posto importante va al **Backup dei dati.** Quando si verificano attacchi che causano il crollo del traffico internet o la perdita di dati, è possibile utilizzare i backup per ripristinare i dati e il funzionamento normale dei sistemi. Tuttavia, è importante ricordare che i backup devono essere protetti adeguatamente per evitare la loro compromissione da parte degli attaccanti. Ciò include l'adozione di misure di sicurezza come la *crittografia* dei dati di backup e la *separazione fisica o logica dei backup dai sistemi di produzione*.

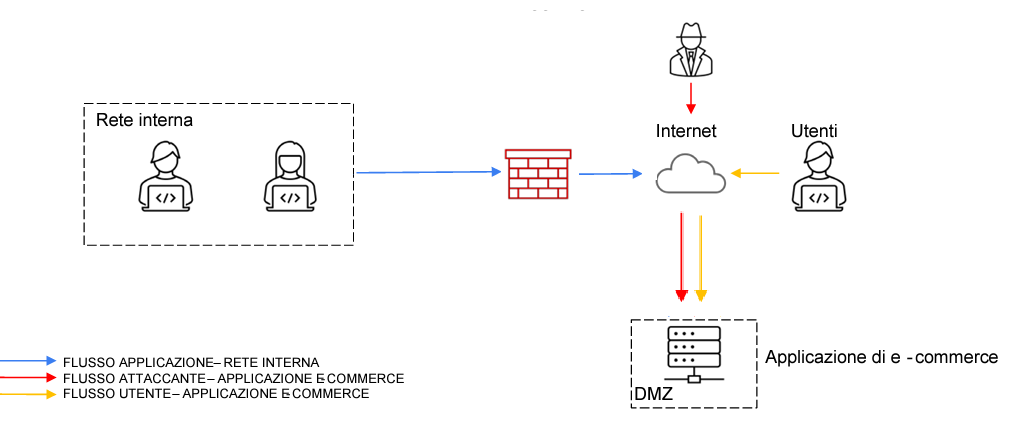
Ma se è efficace per garantire che i dati non vadano persi, non è direttamente coinvolta nella prevenzione dall’attacco stesso. Azioni efficaci in tal senso potrebbero essere:

* Come menzionato in precedenza, un WAF può aiutare a mitigare gli attacchi DDoS bloccando il traffico dannoso prima che raggiunga l'applicazione web;
* Configurazione filtri IP per bloccare o limitare l'accesso a determinati indirizzi IP noti per condurre attacchi DDoS;
* Implementare sistemi di monitoraggio che possano rilevare rapidamente gli attacchi DDoS e attivare procedure di risposta per mitigare l'impatto;
* Pianificazione di risposta agli incidenti. Avere un piano di risposta agli incidenti ben definito che includa procedure per mitigare gli attacchi DDoS e ripristinare rapidamente la disponibilità del servizio.

Implementando queste azioni preventive, è possibile ridurre significativamente il rischio e l'impatto degli attacchi DDoS sull'applicazione e-commerce.

1. Per evitare la propagazione del malware sulla rete interna senza rimuovere immediatamente l'accesso dell'attaccante alla macchina infettata è possibile adottare diverse response:

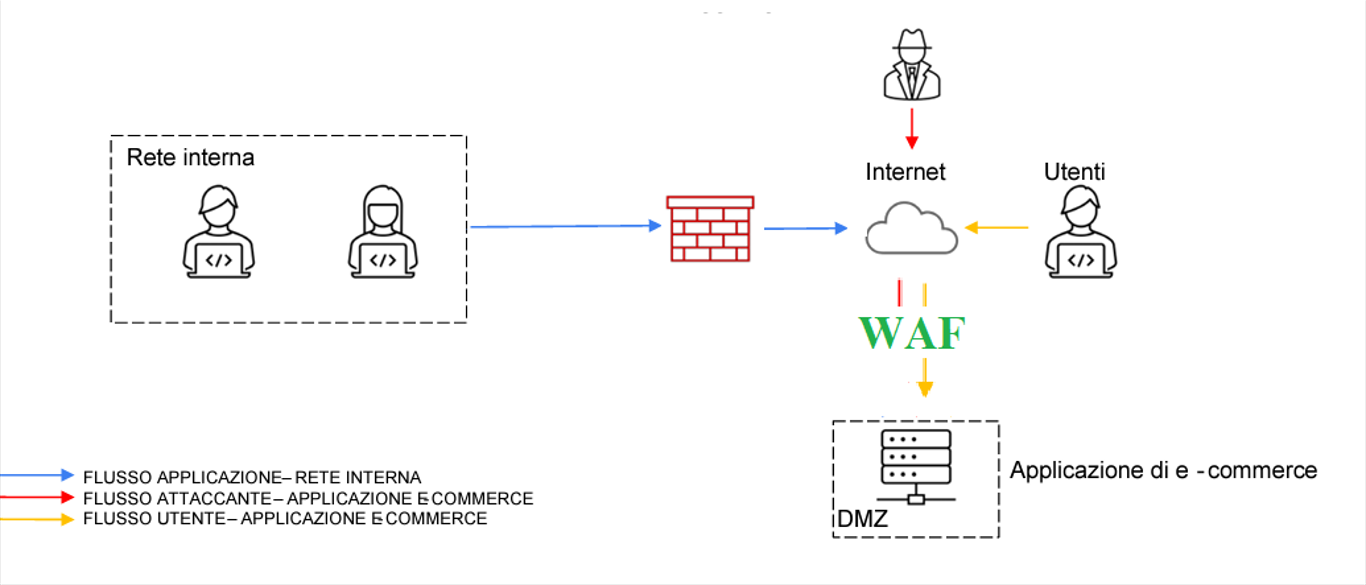
* L'isolamento della macchina infetta è un passo cruciale per prevenire la propagazione del malware sulla rete aziendale. Se possibile, disabilitare temporaneamente le connessioni di rete della macchina infetta per prevenire qualsiasi tentativo di comunicazione con altri dispositivi sulla rete:



* Implementare strumenti di monitoraggio del traffico di rete per rilevare eventuali tentativi di comunicazione sospetti dalla macchina infetta verso altri dispositivi sulla rete.
* Analizzare il malware per comprendere il suo funzionamento e i suoi comportamenti. Questo può fornire informazioni utili per sviluppare contromisure e rilevare attività sospette sulla rete.

Implementando queste response è possibile limitare la propagazione del malware sulla rete e proteggere gli altri dispositivi dalla compromissione, pur consentendo all'attaccante di mantenere l'accesso alla macchina infettata per scopi di monitoraggio e raccolta di informazioni.

1. Soluzione completa:



1. Se si desidera adottare misure più aggressive per isolare la macchina infetta e prevenire la propagazione del malware, si possono considerare alcune azioni più avanzate:

* utilizzare soluzioni di sicurezza avanzate come sistemi di rilevamento delle minacce e prevenzione delle intrusioni (**IDS/IPS**) per monitorare e proteggere la rete da attività malevole;
* **segmentazione** della rete informatica è una pratica cruciale per migliorare la sicurezza e prevenire attacchi informatici. Consiste nel dividere la rete in segmenti più piccoli o "zone", ognuno dei quali ha accesso controllato solo a determinate risorse e servizi;
* utilizzare strumenti di sicurezza **endpoint** avanzati che consentono di isolare automaticamente i dispositivi compromessi dalla rete, impedendo loro di comunicare con altri dispositivi sulla rete;
* estendere l'uso dell'autenticazione **multi-fattore** per aggiungere un ulteriore livello di sicurezza all'accesso agli applicativi e ai dati sensibili, riducendo così il rischio di accessi non autorizzati;
* implementare la **crittografia end-to-end** per proteggere i dati sensibili durante il trasferimento e lo storage, garantendo che siano inaccessibili anche in caso di compromissione della rete o dei dispositivi;
* implementare politiche avanzate di gestione dei privilegi e controllo degli accessi per garantire che solo gli utenti autorizzati possano accedere alle risorse e ai dati sensibili;
* utilizzare **firewall** avanzati che offrono funzionalità di analisi approfondite del traffico, protezione contro attacchi avanzati come gli attacchi a livello di applicazione e capacità di isolamento delle minacce per ridurre la superficie di attacco e mitigare le violazioni di sicurezza;
* un **full backup**, ovvero un tipo di backup che copre l'intero insieme di dati e file presenti su un sistema o su una determinata porzione di esso;

Integrare queste tecnologie avanzate di sicurezza nell'infrastruttura può fornire una protezione più completa e resiliente contro una vasta gamma di minacce informatiche, consentendo di rilevare, mitigare e rispondere prontamente alle violazioni di sicurezza in modo più efficace. Richiedono però notevoli costi, quindi è ovvio che a seconde del budget a disposizione delle aziende, e tenendo conto delle esigenze specifiche, si andrà a valutare l’uno o l’altra delle soluzioni proposte.

Tenendo conto dell’azienda in oggetto del progetto di oggi, e calcolando un budget di 7k, potremmo proporre una segmentazione della rete informatica (4k) con incremento dei sistemi IPS/IDS (3k) che, rientrando nel budget, forniscono un servizio di protezione di un certo livello a costi sostenuti.