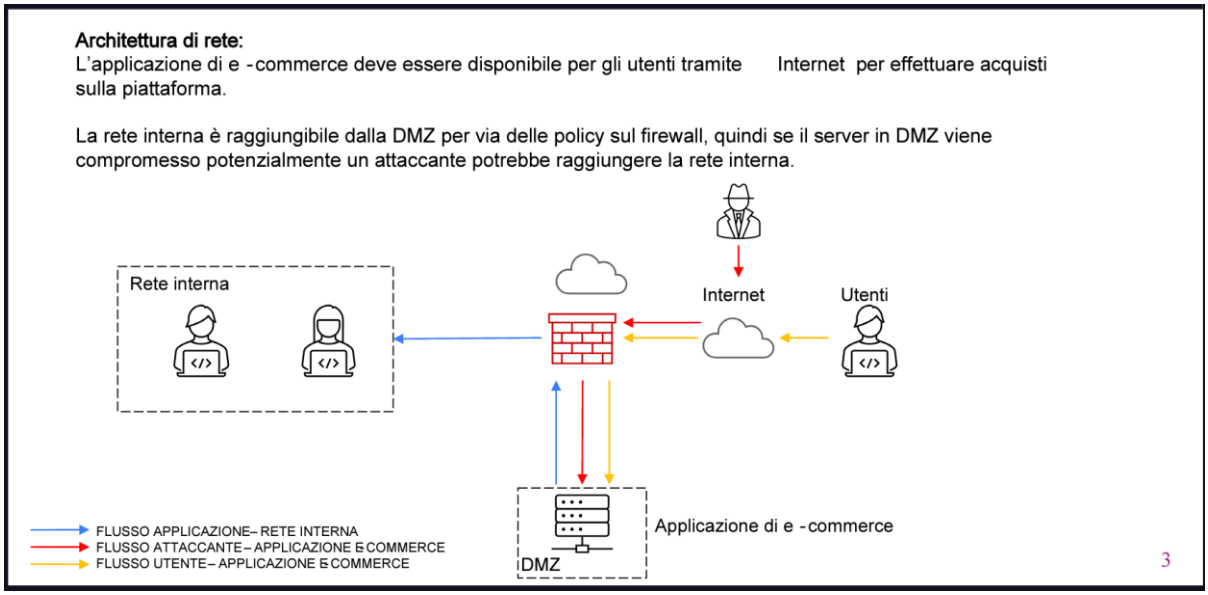
Progetto S9L5

Traccia:

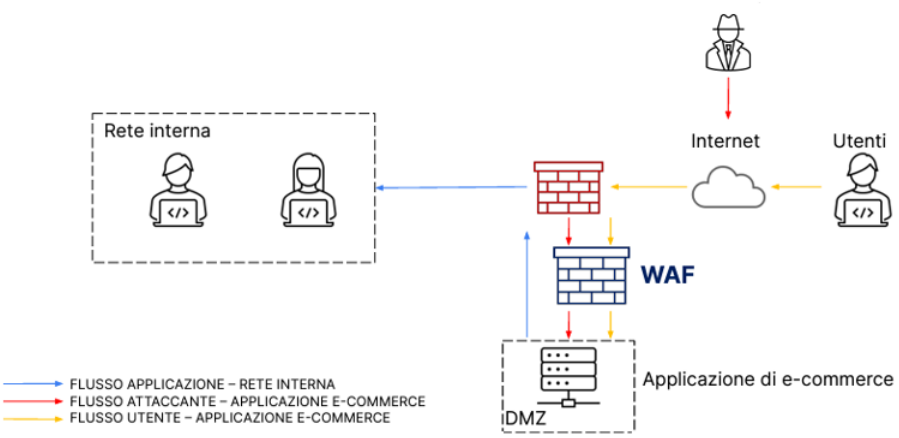


Con riferimento alla figura di rete, rispondere ai seguenti quesiti.

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).

Quesito 1:

Per rafforzare la protezione della Web App dalle minacce XSS e SQLi, oltre all'impiego di un Web Application Firewall (WAF), che filtra il traffico specifico per le applicazioni web, si raccomanda di implementare una serie di best practices di sicurezza. Questo include la sanitizzazione di tutti gli input per prevenire l'esecuzione di codice malevolo, l'uso di prepared statements per le query SQL, la gestione sicura delle sessioni e l'applicazione di una Content Security Policy.



Quesito 2:

L'attacco DDoS ha causato l'indisponibilità della piattaforma di e-commerce per 10 minuti. Presupponendo che gli utenti spendano circa 1.500€ al minuto, possiamo stimare i danni causati dalla perdita di guadagni potenziali sul business moltiplicando la spesa media degli utenti per minuto per i minuti di servizio non disponibile.

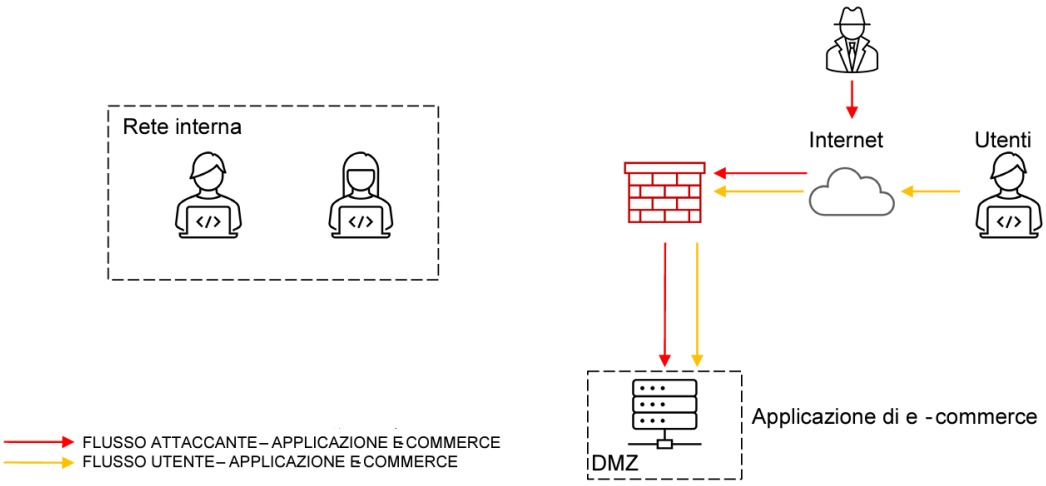
Impatto sul business = 1.500 € x 10 minuti = 15.000 €

In conclusione, per 10 minuti di indisponibilità, l'azienda ha perso 15.000 € di possibili entrate ma l'impatto può essere maggiore considerando la perdita di fiducia dei clienti e potenziali danni alla reputazione.

In futuro per mitigare questo tipo di problema si potrebbero utilizzare dei servizi di mitigazione DDoS forniti da terze parti come un reverse proxy, che possono rilevare e filtrare il traffico malevolo prima che raggiunga l'infrastruttura dell'applicazione.

Quesito 3:

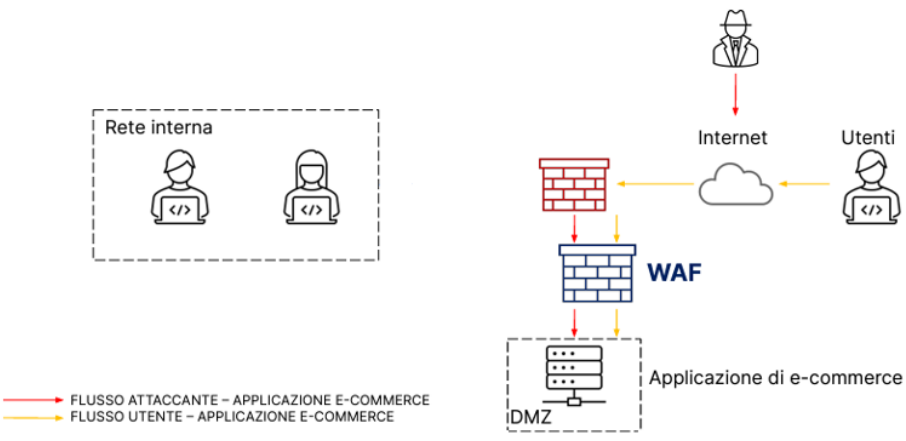
Dando priorità alla sicurezza, si può optare per una strategia che prevede l'isolamento della macchina compromessa. In questa situazione, la macchina sarà direttamente collegata a internet, quindi raggiungibile dall'attaccante, ma non sarà più connessa alla rete interna. La figura nella slide successiva illustra la soluzione adottata, mostrando come la strategia di isolamento impedisca qualsiasi comunicazione tra l'applicazione web e la rete interna.



Quesito 4:

La strategia completa di sicurezza per la Web App unisce misure preventive con un piano di risposta rapida agli incidenti. Prioritizzando la sicurezza, optando per l'isolamento della macchina compromessa, separandola dalla rete interna e collegandola direttamente a internet. Questo impedisce all'attaccante di accedere alla nostra rete interna mentre mantiene la macchina compromessa raggiungibile per ulteriori indagini e rimedi.

Inoltre, per rafforzare ulteriormente la protezione dell'applicazione web da minacce come XSS e SQLi, abbiamo implementato un Web Application Firewall (WAF) che serve da primo livello di difesa, filtrando il traffico specifico per le applicazioni web. Questo è complementare all'adozione di best practices di sicurezza quali la sanitizzazione degli input per neutralizzare codice malevolo, l'impiego di prepared statements per evitare iniezioni SQL, la gestione sicura delle sessioni per proteggere l'identità e i dati degli utenti e l'applicazione di una Content Security Policy per limitare le risorse esterne eseguibili sul sito web.



Quesito 5:

Come strategia di rafforzamento dell'infrastruttura possiamo includere l'implementazione di un sistema di bilanciamento del carico (reverse proxy) con mitigazione DDoS integrata, per una robusta difesa contro gli attacchi esterni. Aggiungeremo inoltre un Web Application Firewall (WAF) per filtrare il traffico in ingresso all'applicazione web e stringeremo le policy del firewall per limitare l'accesso alla DMZ ai soli servizi essenziali. Queste misure assieme andranno a creare una barriera sicura e resiliente.

Bonus

Bonus: Analizzare le seguenti segnalazioni caricate su anyrune fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

1. https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/
2. https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

Primo link:

La prima segnalazione denominata "PERFORMANCE_BOOSTER_v3.6.exe", è stato classificato come un'attività malevola. Questo file è un eseguibile per Windows e presenta vari indicatori che suggeriscono la sua natura malevola come il poter modificare le impostazioni di sicurezza della PowerShell, creare nuovi file pericolosi e usare comandi per alterare il sistema. Per proteggersi da attacchi simili in futuro, è molto importante non aprire file che vengono da siti o persone di cui non ci si fida o da fonti non verificate o sospette.

Secondo link:

La seconda segnalazione che abbiamo esaminato mostra che c'è stata un'attività malevola attraverso l'esecuzione di file sospetti, come "MicrosoftEdgeUpdate.exe" e "iexplore.exe". Questi comportamenti includono azioni come il disabilitare le protezioni di sicurezza, avviarsi da posizioni non normali, modificare la pianificazione di alcune attività e aggiungere voci per disinstallare software. È fondamentale prendere precauzioni come mantenere il software sempre aggiornato, educare gli utenti sulla sicurezza informatica, utilizzare strumenti di sicurezza avanzati e navigare in modo sicuro per proteggersi da attacchi di questo tipo.