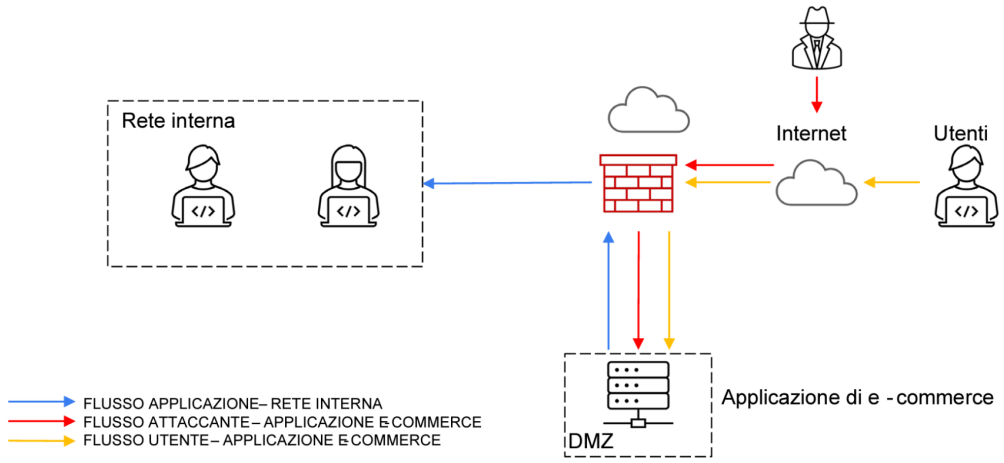
S9/L5 - 26 aprile 2024 - Gianmarco Mazzoni

Consegna: *Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.*

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.

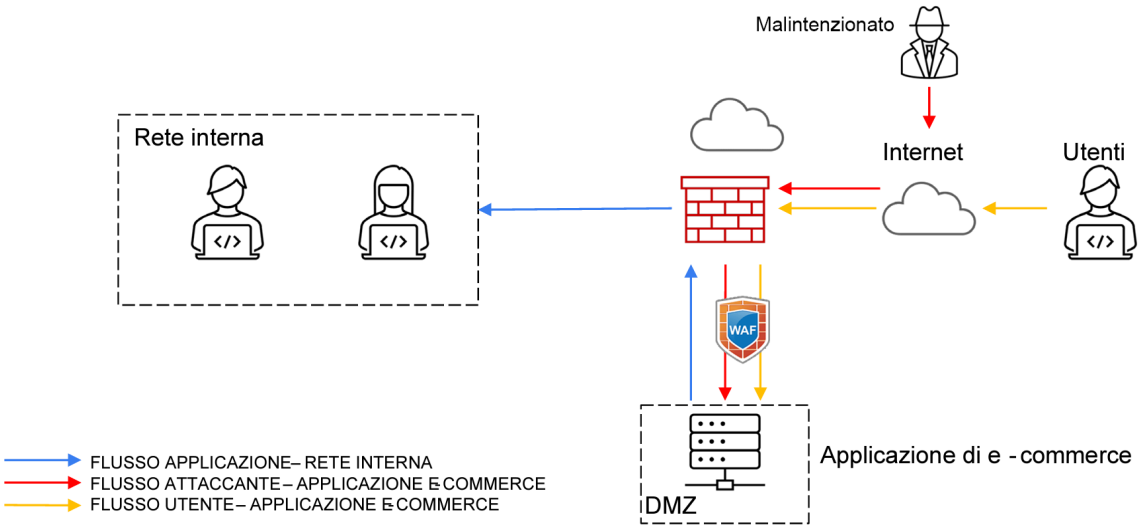


1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.
2. Impatti sul business : l'applicazione Web subisce un 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 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.
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).

1. Azioni preventive

Per aggiungere un layer di sicurezza molto importante all'azienda, utilizzerei un WebApp Firewall per filtrare il traffico in entrata e uscita e bloccare le connessioni non autorizzate, per prevenire i tipi attacchi più noti.

Configurazione con WAF installato:



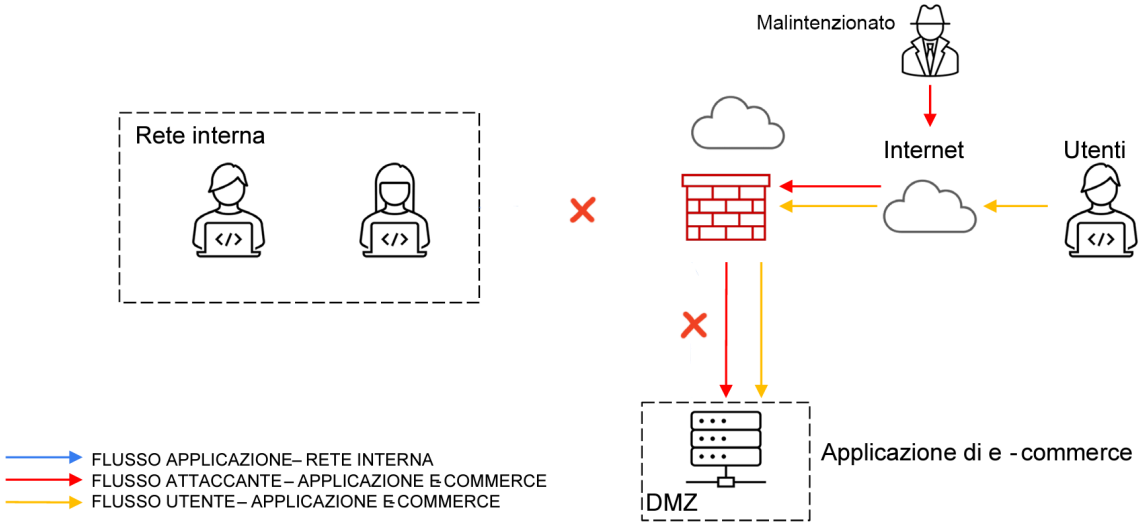
2. Impatti sul business

Nell'ipotesi di un attacco DDoS, sarebbe stato conveniente appoggiarsi sul WAF.
Considerando un caso di indisponibilità del servizio, eseguo un calcolo per stimare i potenziali acquisti perduti.
Spesa media/minuto = 1500.00 EUR
Downtime = 10 minuti

Spesa media/minuto	1500
Downtime	10
Moltiplica	
Perdita totale potenziale	**15000 (EUR)**

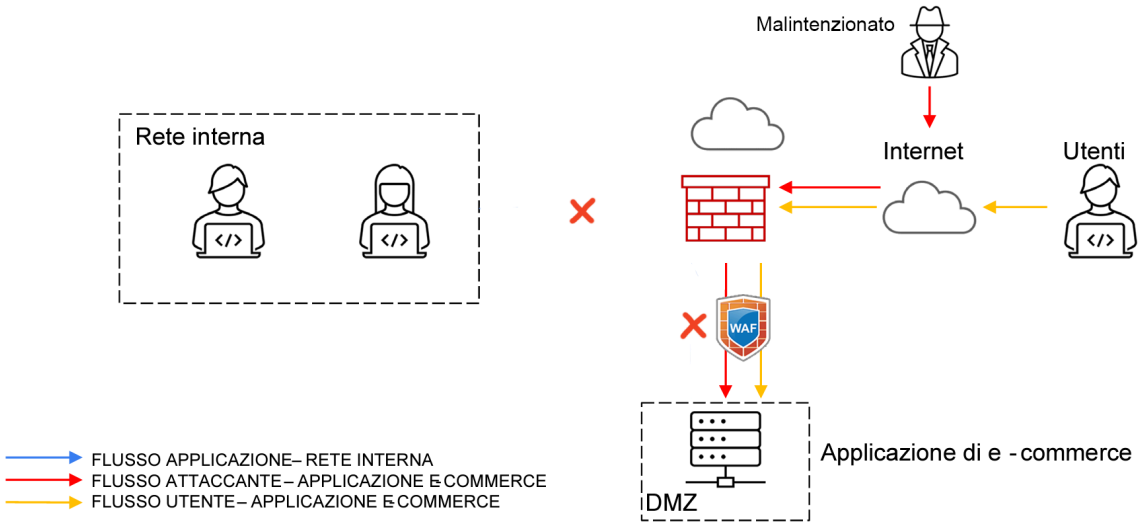
3. Response

Dopo che è stata infettata l'applicazione è necessario isolare la rete interna.
Ho modificato lo schema principale, implicando che il WAF non fosse presente.



4. Soluzione completa

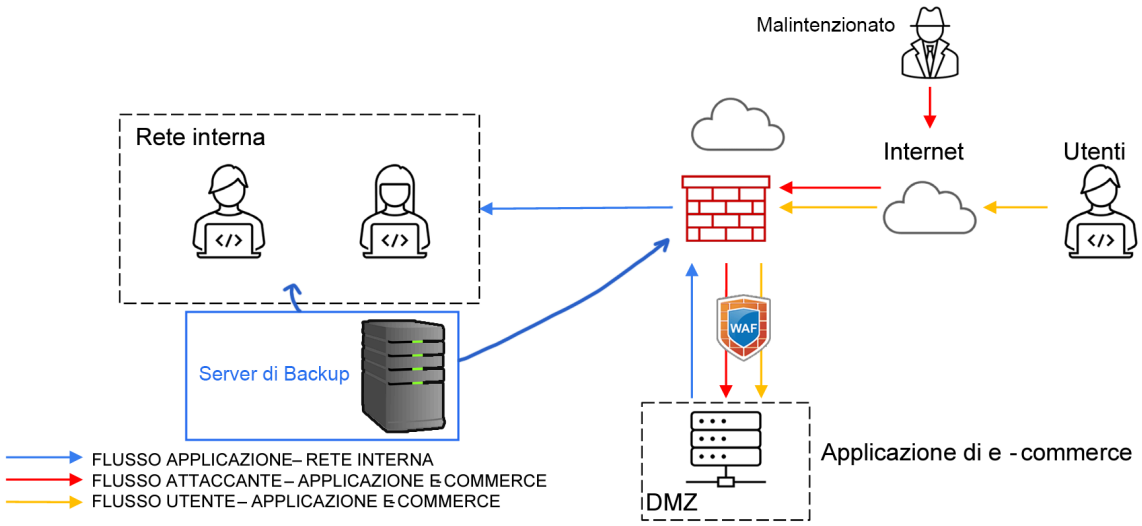
Unendo le due soluzioni, preventive e di response, si può raggiungere uno schema di questo tipo, che includa il WAF piazzato tra il firewall aziendale del Punto 1 e isolando la rete interna.



5. Modifica «più aggressiva» dell'infrastruttura

In caso di budget poco ristretti, ci sono diverse migliorie che si possono apporre al sistema.

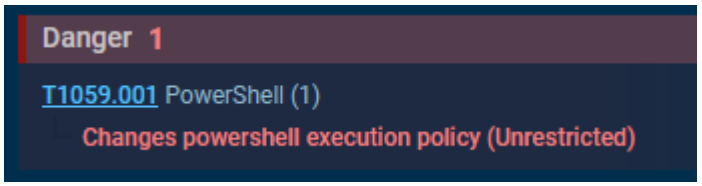
Per esempio l'**installazione di un antivirus** per la rete aziendale proteggerebbe la rete dalle infezioni da malware, che possono essere utilizzati per lanciare attacchi SQLi e XSS.
Il **supplemento di un IDS** invece monitorerebbe il traffico di rete per rilevare attività sospette, che potrebbero indicare attacchi di diverso tipo, come DoS).
Installare **server di backup** impostati con strategia di tipo "Full" o "Incremental" con cui fare interagire la rete interna, e permettere lo svolgimento delle operazioni di recovery, dando anche la possibilità di eseguire dei merge dei dati dopo aver eliminato la minaccia.



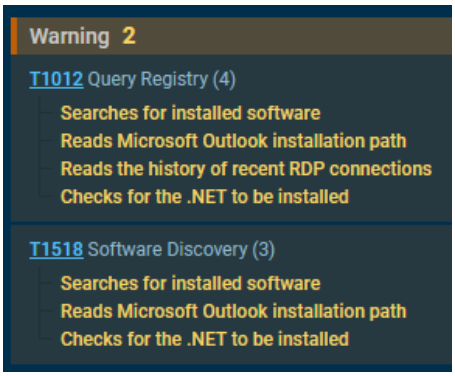
Bonus: Analisi del Malware

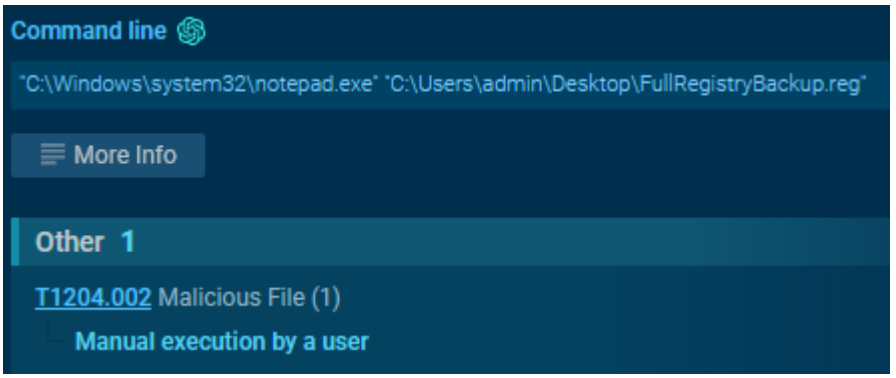
Entrambi i malware listati sono degli Spyware, il cui compito è principalmente la raccolta di informazioni, solitamente in modo indiscreto dall'Utente.

Questo primo malware modifica delle policy di esecuzione della powershell dopo l'avvio.



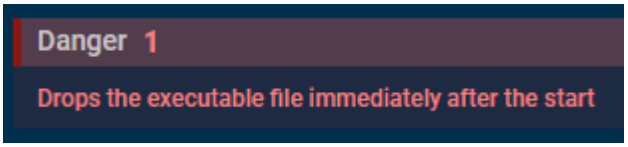
Dopo di che inizia a raccogliere e salvare informazioni di sistema, fingendosi un backup.





Il secondo malware nasconde dietro l'interfaccia che può sembrare innocente e di firma Microsoft, il download di un file da una fonte non esattamente attendibile.

Questo file "droppa" eseguibili Microsoft e si sostituisce a quelli ufficiali.



Disabilita anche il SEHOP (Structured Exception Handler Overwrite Protection), permettendo quindi la sovrascrittura di blocchi di codice responsabili della gestione delle eccezioni, insieme ad altri comportamenti anomali.