

Analisi dei Log

Progetto S9L5 di Ciaschini Giorgio

Indice

- Traccia
- Azioni preventive
- Azioni preventive - WAF
- Impatti sul business
- Response
- Soluzione completa
- Modifica “più aggressiva”
- Bonus 1
- Bonus 2



TRACCIA

Con riferimento alla figura nella prossima slide, rispondere ai seguenti quesiti.

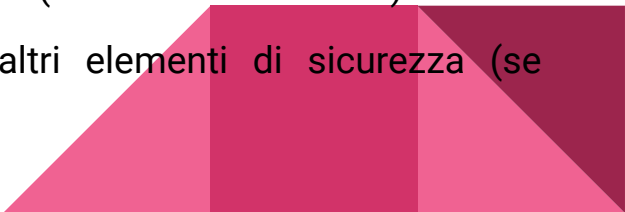
1. **Azioni preventive** : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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 4 con la soluzione proposta.

4. **Soluzione completa** : unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)

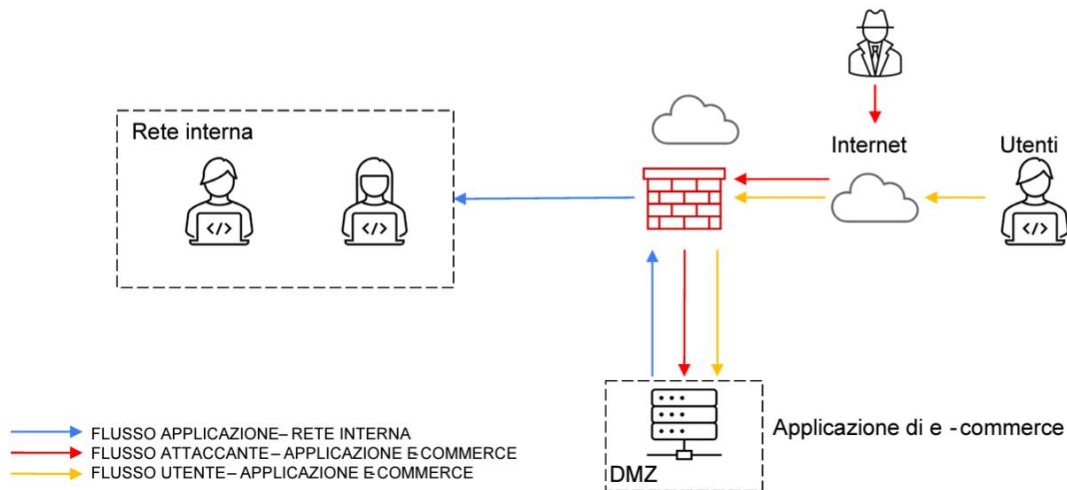
5. **Modifica "più aggressiva"** dell'infrastruttura integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)



TRACCIA

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.



TRACCIA

BONUS:

Analizzare le seguenti segnalazioni caricate su anyrun 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:

<https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>

<https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>



AZIONI PREVENTIVE

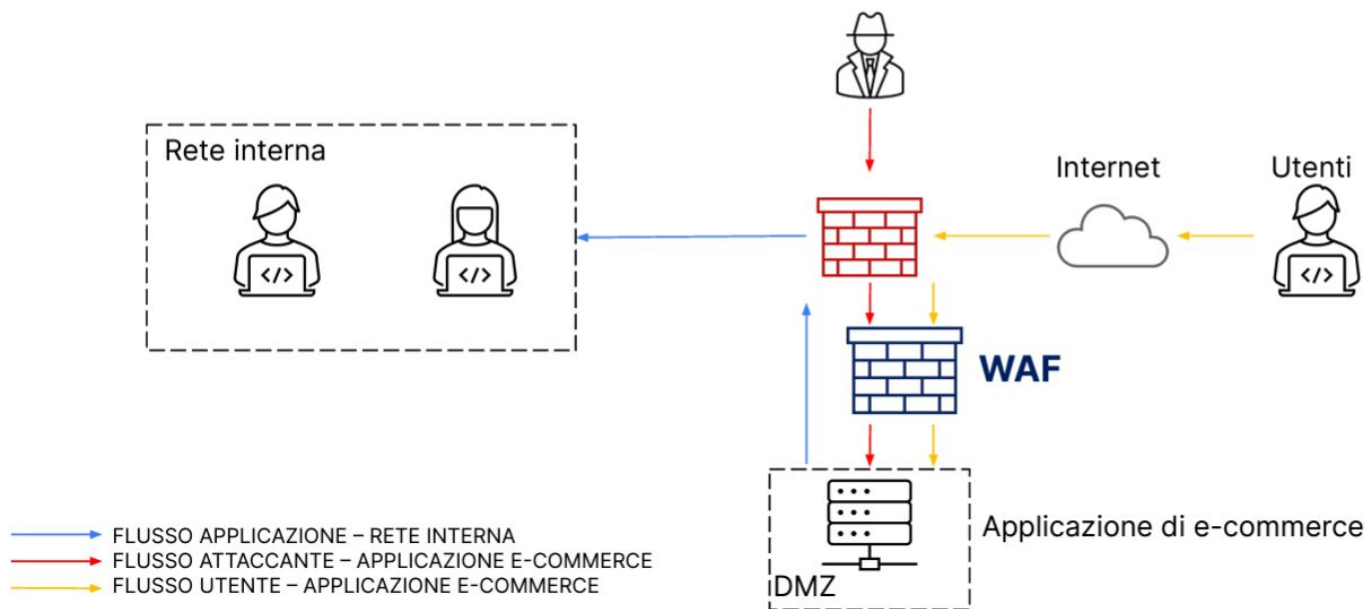
Per garantire la sicurezza delle web application contro le minacce di XSS e SQLi, è consigliabile impiegare preventivamente una Web Application Firewall (WAF).

Un Web Application Firewall (WAF) è una forma di protezione avanzata per le web application. Si colloca tra la web application stessa e gli utenti che vi accedono, come i browser web. La sua funzione principale è quella di analizzare il traffico HTTP in entrata e in uscita per individuare e bloccare potenziali minacce alla sicurezza, come nel nostro caso, attacchi di Cross-Site Scripting (XSS) e SQL injection (SQLi).

Il WAF utilizza regole predefinite e personalizzabili per identificare comportamenti sospetti o pattern di attacco noti. Può quindi intervenire per bloccare il traffico dannoso prima che possa danneggiare la web application. In questo modo, il WAF fornisce un'efficace barriera difensiva contro una vasta gamma di minacce online, proteggendo la web application e i dati degli utenti da potenziali attacchi.



AZIONI PREVENTIVE - WAF



Come possiamo notare nella figura di fianco, il WAF blocca solamente l'attaccante.

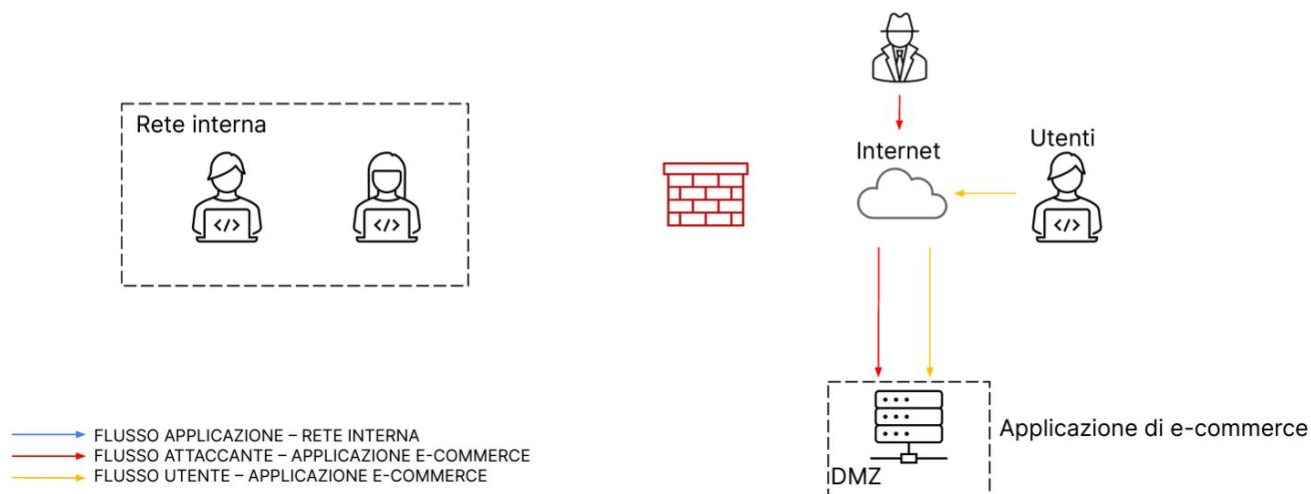
IMPATTI SUL BUSINESS

L'attacco di tipo DDoS ha provocato l'inaccessibilità della piattaforma di e-commerce per un periodo di 10 minuti. Sapendo che gli utenti spendono approssimativamente 1500€ al minuto, possiamo calcolare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1500€) per il numero di minuti di indisponibilità del servizio (10).

In questo caso, i danni stimati sarebbero pari a 15.000€ per 10 minuti di indisponibilità del servizio.

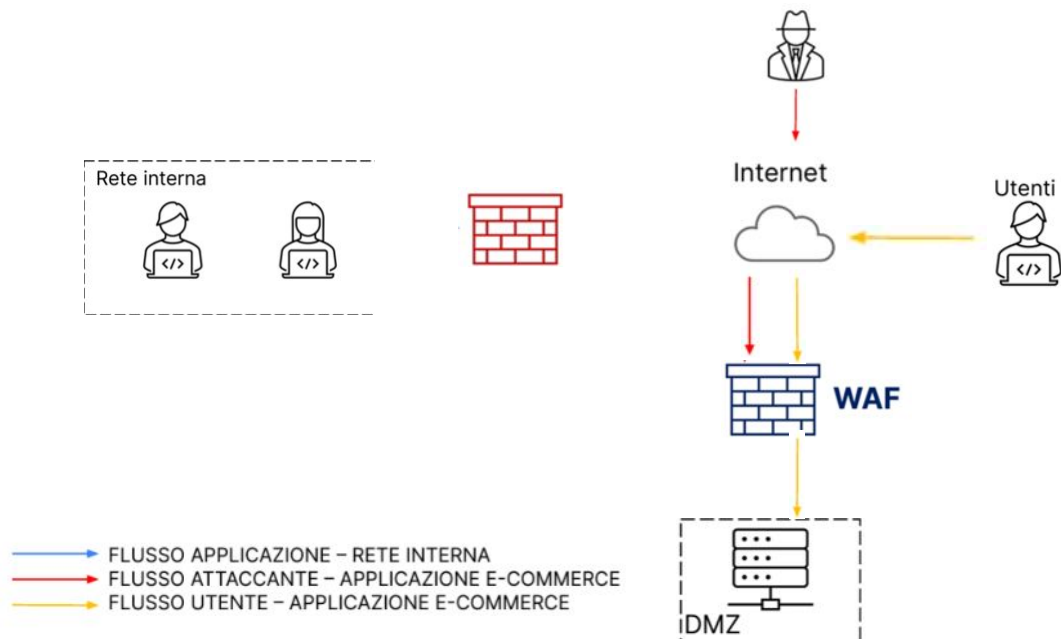


RESPONSE



Abbiamo scelto di adottare l'isolamento come principale strategia per progettare l'integrazione della rete interna dell'azienda. Questo approccio implica la separazione dell'applicazione web dal resto dell'infrastruttura aziendale, riducendo così il rischio di diffusione del malware nell'intera rete. È importante sottolineare che, nonostante l'isolamento, un attaccante che ha ottenuto accesso all'applicativo web dell'e-commerce potrebbe mantenere tale accesso, costituendo così una potenziale minaccia per la sicurezza.

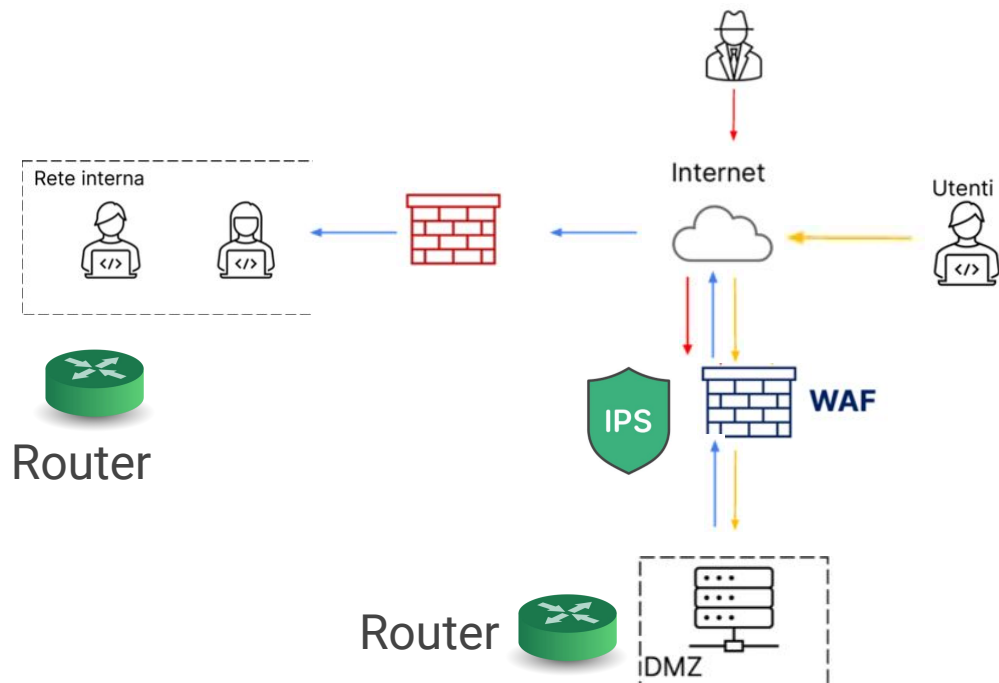
SOLUZIONE COMPLETA



Come possiamo notare nella soluzione completa il WAF blocca l'attaccante dalla DMZ e isolando la rete interna abbiamo modo di evitare che si diffonda il malware.

MODIFICA PIÙ AGGRESSIVA

- FLUSSO APPLICAZIONE – RETE INTERNA
- FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
- FLUSSO UTENTE – APPLICAZIONE E-COMMERCE



Per rafforzare la sicurezza dell'e-commerce, abbiamo installato un sistema IPS direttamente nel Web Server, che monitora e blocca intrusioni e attacchi. Inoltre, abbiamo diviso l'infrastruttura in sottoreti per migliorare la gestione della rete e isolare le componenti, aumentando la resilienza alle minacce esterne.

BONUS 1

- Cos'è il "Performance_booster_v3.6.exe"?
È un file eseguibile che sembra migliorare le performance del computer.
- Cosa fa realmente?
Rilascia il file eseguibile immediatamente dopo l'avvio e modifica la policy di esecuzione della powershell.
- Soluzione:
una possibile soluzione è rimuovere immediatamente il file.



BONUS 1

MALICIOUS

Changes powershell execution policy (Unrestricted)

- cmd.exe (PID: 668)

Drops the executable file immediately after the start

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

SUSPICIOUS

Starts CMD.EXE for commands execution

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Using PowerShell to operate with local accounts

- powershell.exe (PID: 3332)

Starts POWERSHELL.EXE for commands execution

- cmd.exe (PID: 668)

Executing commands from a ".bat" file

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Checks for the .NET to be installed

- regedit.exe (PID: 2824)

Reads the Internet Settings

- powershell.exe (PID: 3332)

Reads Microsoft Outlook installation path

- regedit.exe (PID: 2824)

Searches for installed software

- regedit.exe (PID: 2824)

Runs PING.EXE to delay simulation

- cmd.exe (PID: 668)

Reads the history of recent RDP connections

- regedit.exe (PID: 2824)

Uses ATTRIB.EXE to modify file attributes

- cmd.exe (PID: 668)

Nello screenshot a fianco possiamo notare il report che ci viene rilasciato da “anyrun” dove sono messe in evidenza le caratteristiche del Malware.



BONUS 2

- Cos'è "iexplore.exe"?
Sembra un file eseguibile di internet explorer.
- Cosa fa realmente?
Rilascia il file eseguibile immediatamente dopo l'avvio e viene eseguito proprio come un software windows e quindi modificare servizi importanti.
- Soluzione:
una possibile soluzione è scansionare il sistema e rimuovere immediatamente il file.



BONUS 2

MALICIOUS

Drops the executable file immediately after the start

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

SUSPICIOUS

Process drops legitimate windows executable

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Executable content was dropped or overwritten

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

Starts a Microsoft application from unusual location

- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Disables SEHOP

- MicrosoftEdgeUpdate.exe (PID: 4040)

Starts itself from another location

- MicrosoftEdgeUpdate.exe (PID: 4040)

Creates/Modifies COM task schedule object

- MicrosoftEdgeUpdate.exe (PID: 4012)

Creates a software uninstall entry

- MicrosoftEdgeUpdate.exe (PID: 4040)

Reads the Internet Settings

- MicrosoftEdgeUpdate.exe (PID: 3408)

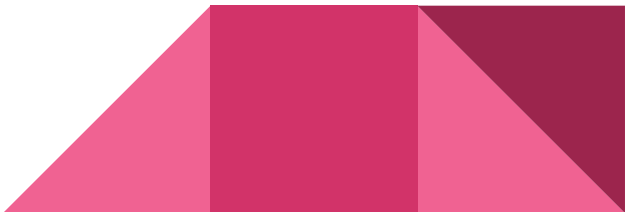
Reads settings of System Certificates

- MicrosoftEdgeUpdate.exe (PID: 3408)

Checks Windows Trust Settings

- MicrosoftEdgeUpdate.exe (PID: 3408)

Come vediamo dallo screenshot di fianco, abbiamo un dettagliato report, dove vengono evidenziate le caratteristiche del malware.





GRAZIE