REPORT

S9 - L5

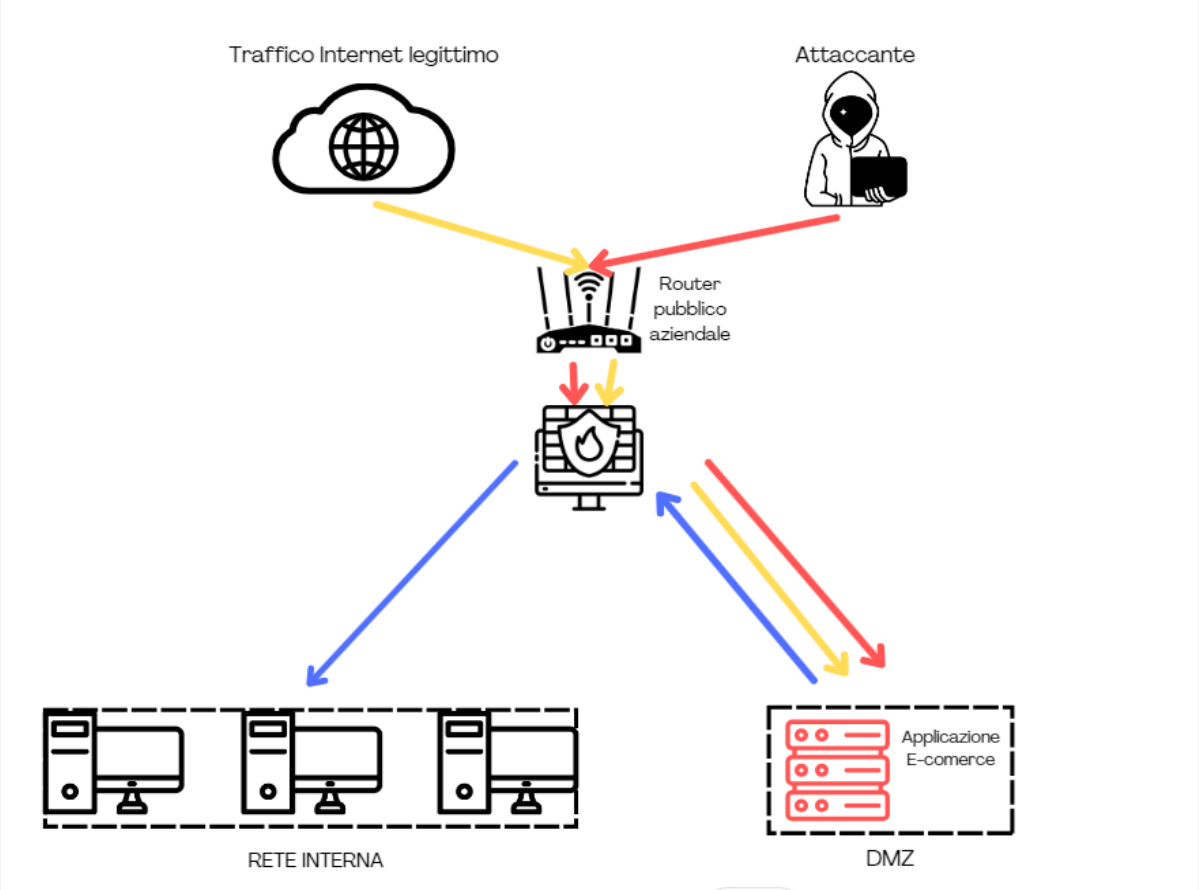
Pablo Ballesteros

Indice

Debriefing | Architettura di rete

L'azienda Theta offre servizi di e-commerce a utenti e clienti via Internet su un server dedicato che funziona come la Demilitarized zone (DMZ) della rete aziendale. La configurazione di rete non consente al traffico proveniente da Internet di entrare nella rete interna, il che rappresenta una buona pratica di sicurezza.

Tuttavia, la rete aziendale è configurata in modo che il traffico originario dalla DMZ possa entrare nella rete interna (che dovrebbe essere accessibile solo agli dispositivi dentro di se stessa). Ciò suggerisce una possibile infiltrazione da parte di un utente Internet malintenzionato che riesca a intercettare e modificare tali comunicazioni, o che riesca a compromettere il server web dell'e-commerce all'interno della DMZ.



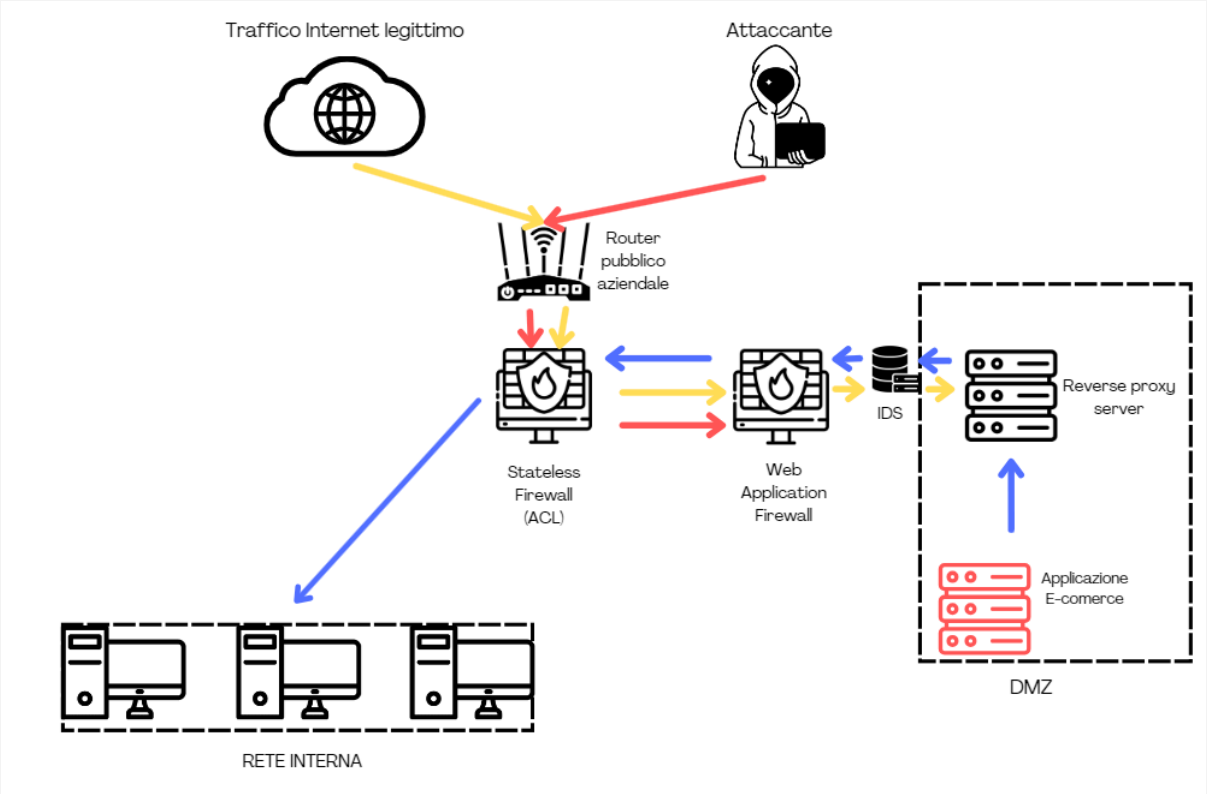
Debriefing | DMZ

Una DMZ, o "zona smilitarizzata", è una rete separata e protetta di computer o dispositivi che si trova tra la rete interna di un'organizzazione e una rete esterna, come Internet. La DMZ funge da ulteriore livello di sicurezza consentendo l'accesso a determinati servizi dall'esterno, mantenendo isolata la rete interna.

La Theta DMZ contiene il server web. Sfortunatamente, i server web, essendo apertamente esposti a Internet, sono suscettibili agli attacchi SQL injection o Cross Site Scripting (XSS). Questi attacchi potrebbero garantire l'accesso o la manipolazione di un server web.

Azione preventive

Esistono diverse misure che possono essere adottate per ridurre il rischio di un attacco diretto al server web e-commerce. Il primo sarebbe l'implementazione di un **Web Application Firewall (WAF)**. Questi firewall sono progettati specificamente per proteggere dagli attacchi XSS, DoS, DDoS e SQLi. Se volessi ridurre il contatto diretto tra il traffico Internet e il server web, si potrebbe implementare un **server proxy inverso**, che fungerà da sorta di intermediario tra il server web e Internet. Finalmente, un Intrusion Detection System fronte al server web avviserà agli amministratori di rete di qualsiasi attività sospetta.



In questa immagine vediamo la configurazione della rete con gli accorgimenti implementati. Come puoi vedere, l'attaccante non può andare oltre il WAF, ma anche se lo facesse, accederebbe solo al server proxy inverso, quindi non avrebbe accesso al server web reale.

Scenario DDoS | Impatto sul business

Uno o più hacker sono riusciti a penetrare le difese e hanno sferrato un attacco DDoS al server web, rendendo il sito web inaccessibile agli utenti. Il sito web è rimasto offline per 10 minuti, se ogni minuto per Theta vengono generati 1.500 euro, ciò rappresenta una perdita potenziale di 15.000 euro, oltre a una piccola perdita di reputazione.

Scenario infezione malware | isolazione

Un utente malintenzionato ha introdotto malware nel nostro server web, ma seguendo la configurazione di rete suggerita nella sezione “Azione preventive” di questo documento, possiamo facilmente isolare le comunicazioni, eliminando ogni rischio che l'utente malintenzionato possa comunicare con la rete interna, pur mantenendo una connessione con e possiamo analizzare l'attività.

Raggiungeremo questo obiettivo configurando un firewall stateless
(dentro il router, con "packet filtering" attraverso un elenco di controllo degli accessi. Utilizzando questa lista di controllo degli accessi possiamo semplicemente negare tutto il traffico proveniente dal server diretto verso la rete interna.