CYBERSECURITY ANALYSIS

Analisi di Sicurezza Aziendale

MARCO MALIZIA

Presentazione di una proposta di aggiornamento di sicurezza destinato ad una situazione aziendale critica.

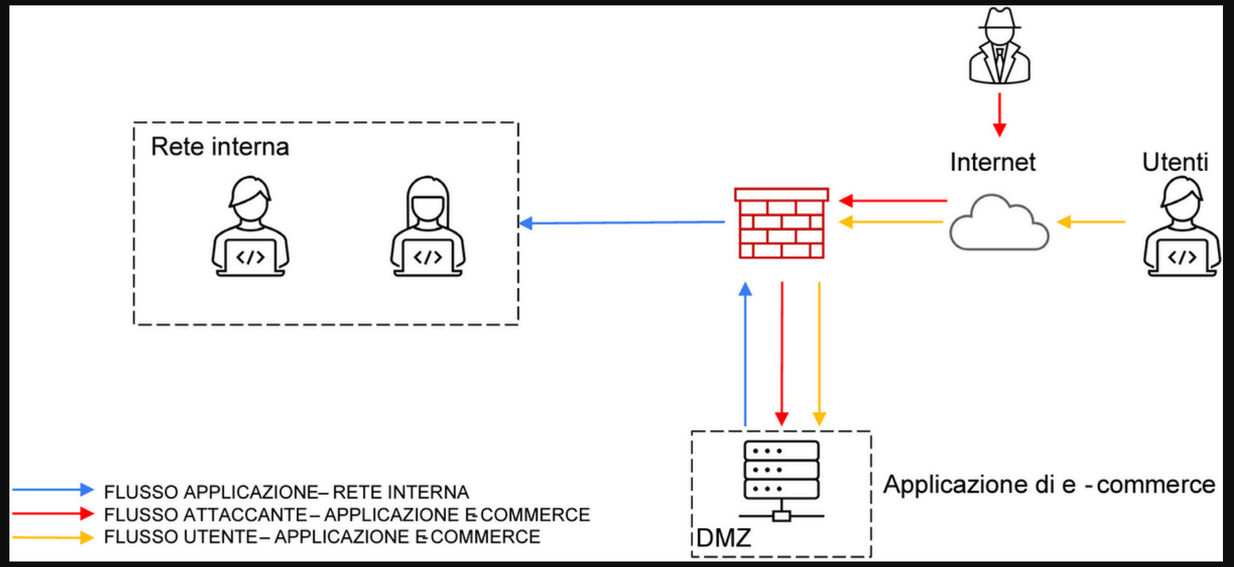
indice

Analisi situazione aziendale

Nello schema raffigurato possiamo visionare lo schema della configurazione di rete aziendale oggetto di analisi, come possiamo notare sono presenti:

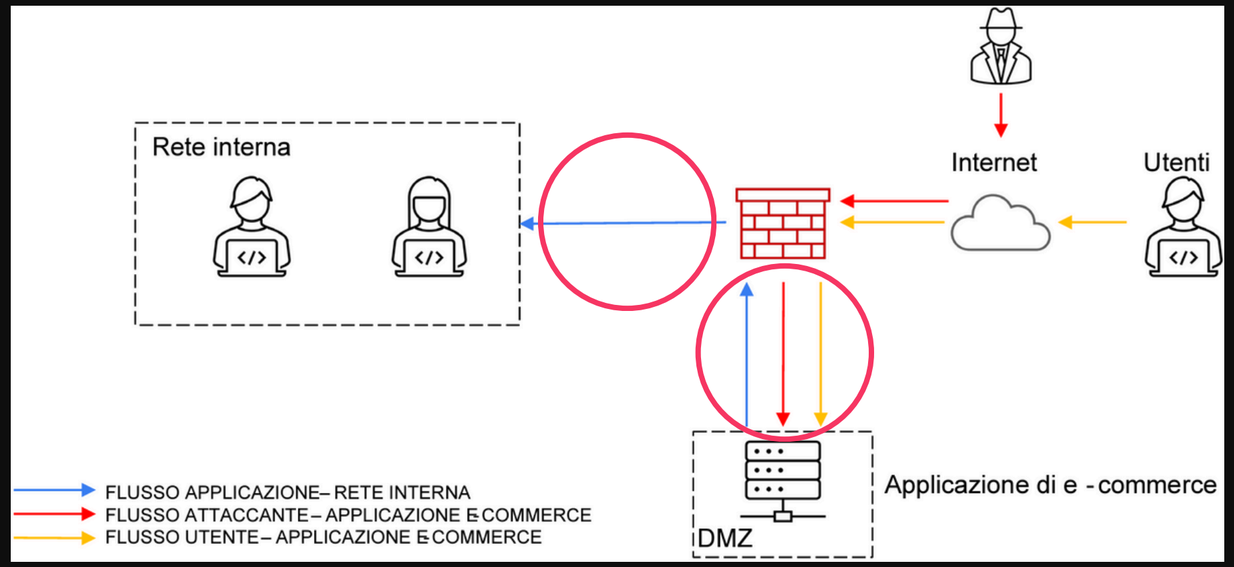
- rete interna destinato ai dipendenti aziendali
- rete dmz destinata all'applicazione e-commerce
- un firewall posizionato tra azienda ed internet
- raffigurazione di cliente ed attaccante che si collegano attraverso internet.

Grazie all'aiuto delle frecce colorate possiamo capire il traffico attraverso la rete e possiamo valutarne la situazione, la criticità è rappresentata dalla possibilità dell'attaccante di poter accedere facilmente alla rete dmz destinata all' applicazione, andiamo a risolvere aumentando la sicurezza.



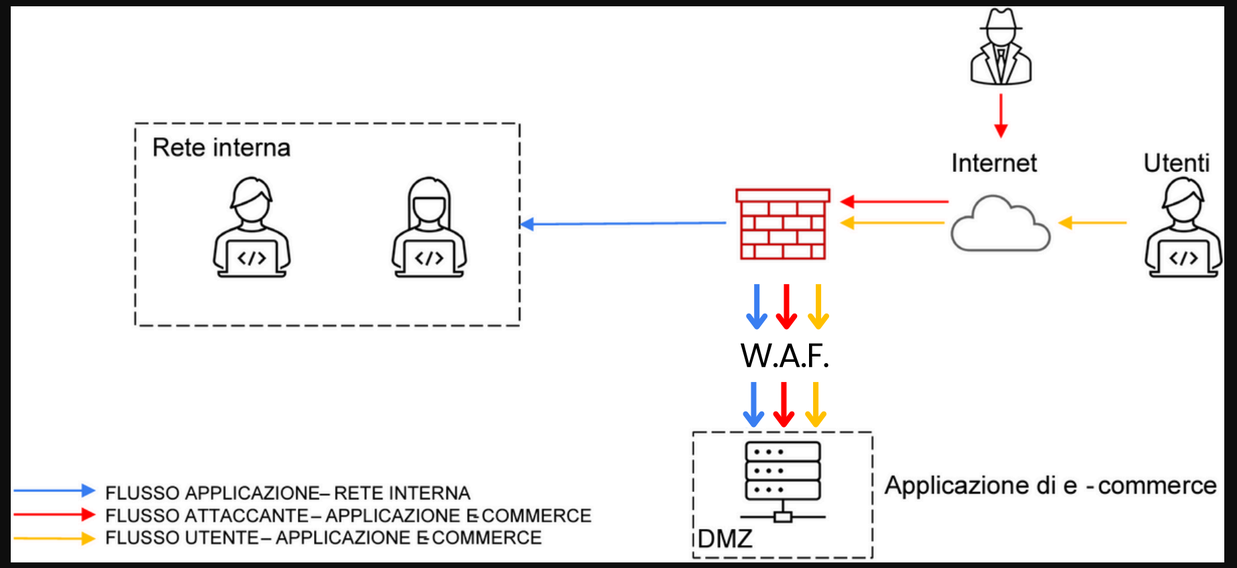
Analisi problematiche di rete

Una delle problematiche, vista la situazione, riguarda la sicurezza dell'e-commerce che risulta molto vulnerabile a qualsiasi tipo di attacco.
Soffermandoci sullo schema di rete possiamo intuire che, non essendoci un firewall dedicato alla rete dmz contenente l'e-commerce, potrebbero verificarsi attacchi di tipo SQLi e XSS che comprometterebbero in modo significativo la situazione aziendale.
Un altra vulnerabilità vede come oggetto l'intera rete aziendale, nel caso di diffusione Malware, la possibilità che si propaghi a tutti i device risulta molto semplice e significativa, con delle conseguenze notevoli che comprometterebbero molto la sicurezza e la situazione aziendale oggetto.



Soluzione vulnerabilità e-commerce

La prima modifica per implementare la sicurezza della rete riguarda l'aggiunta di un Web Application Firewall posizionato di fronte all'e-commerce cosi da garantire dei canoni di sicurezza maggiori, il dispositivo in questione è specializzato nella difesa di applicazioni da attacchi SQLi e XSS.



Possibili impatti sul business

Ipotizziamo adesso una situazione in cui l'azienda si trovasse difronte ad un'attacco DDoS che blocca ogni tipo di servizio disponibile.
Possiamo aggiungere alcuni fattori per rendere tangibile la possibile criticità quali, la durata dell'attacco, ipotizziamo 10 minuti e la situazione lavorativa con effettivo guadagno, prendiamo come per esempio una situazione fiorente con circa 1200€ al minuto.
Il calcolo per la perdita totale è molto semplice perchè basta moltiplicare l'incasso al minuto x i minuti di inattività, quindi

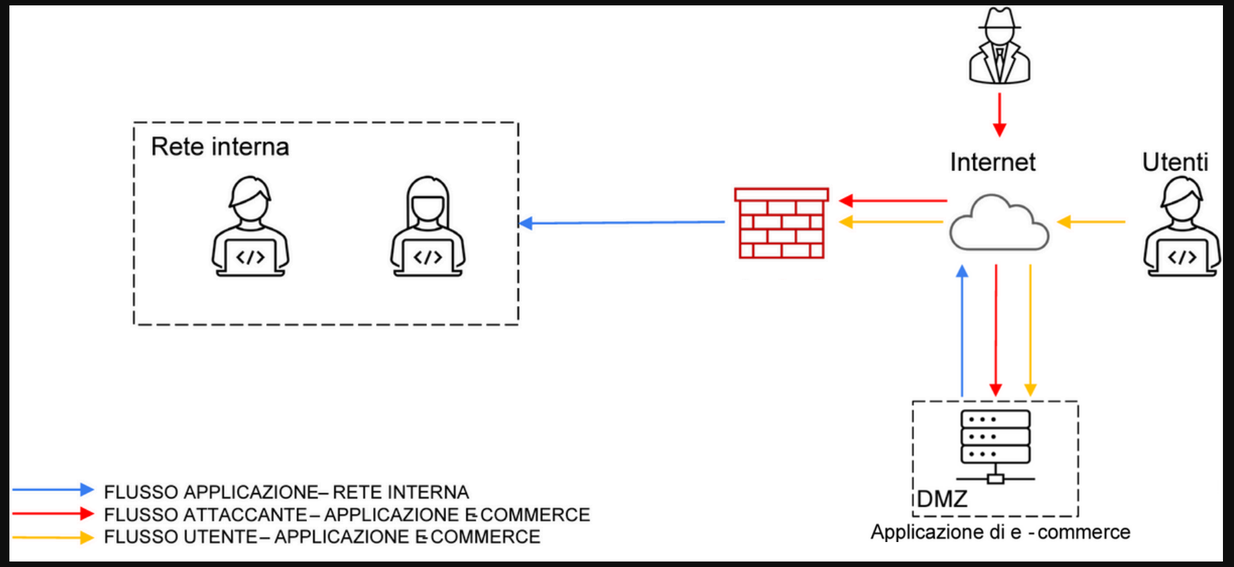
- Perdita totale = incasso al minuto x minuti di inattività
- Perdita totale = 1200€/min x 10min = 12000€

Con i numeri davanti possiamo visualizzare in modo ancora più nitido la criticità ed ipotizzare la proposta di incremento dei canoni di sicurezza.
Si consiglia l'aggiunta di un device destinato alla mitigazione degli attacchi DDoS, le proposte sono molte ma vorremmo consigliare:

- Cloudflare, che offre servizi che sono progettati per bloccare gli attacchi DDoS su larga scala,
- AWS Shield, servizio offerto da Amazon Web Services che offre due pacchetti, Standard: servizio incluso senza costi aggiuntivi e fornisce protezione automatica contro la maggior parte degli attacchi DDoS comuni e Advanced: che offre protezione aggiuntiva e un maggiore livello di supporto e mitigazione.

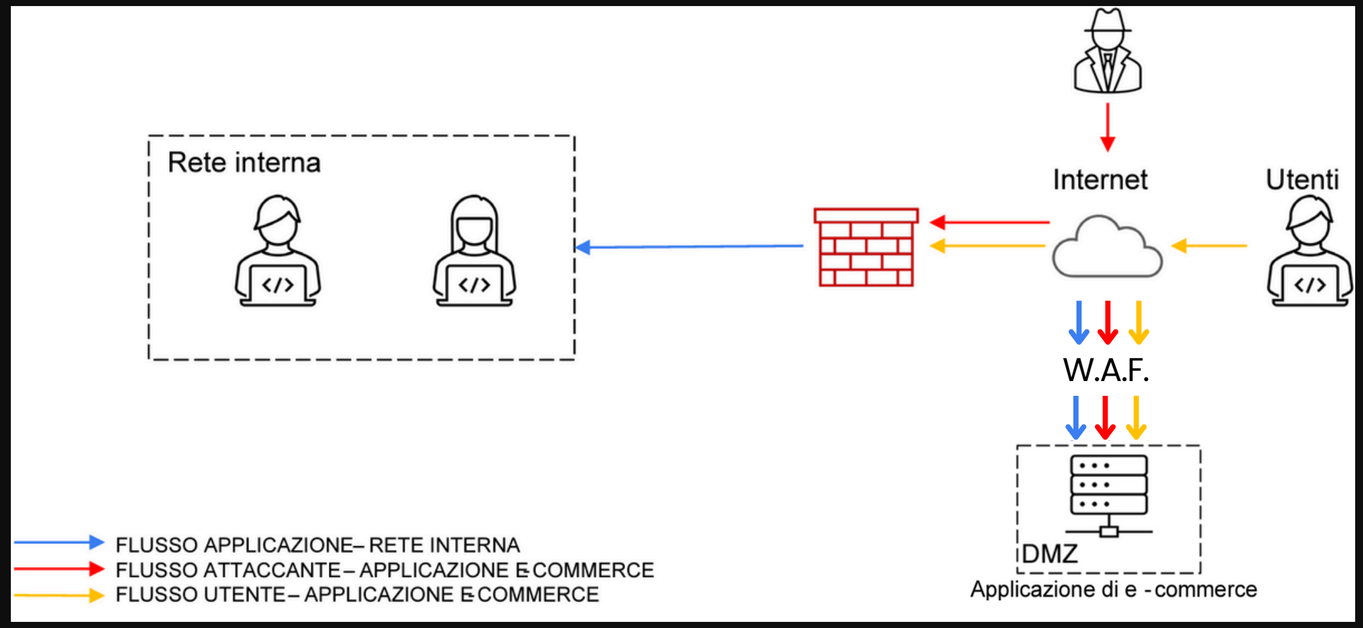
Isolamento
Malware

Analizziamo ora una possibile situazione di infezione della rete dmz destinata all'e-commerce con un **Malware**, la situazione che si andrebbe a creare risulterebbe molto critica per l'intera rete, perciò, bisogna subito intervenire per evitare che il **Malware** si propaghi ed infetti ogni device componente la rete.
La soluzione che consigliamo prevede lo spostamento della web app al di fuori del firewall di rete, cosi da schermare le informazioni di rete della rete interna destinata ai dipendenti ed inoltre di evitare il **pivoting** dell'attaccante, ovvero, di usare la macchina infetta come base per possibili attacchi, effettuando questa modifica possiamo comunque accedere alla web app, limitando però il traffico inverso vista la protezione del firewall di rete configurato in precedenza.



Proposta soluzione ottimale

Viste le situazioni viste in precedenza vorremmo consigliare la soluzione che rappresenta la configurazione di sicurezza ottimale per l'azienda, impostando la rete come nello schema raffigurato, i canoni di sicurezza risulteranno importanti e con maggiore efficienza.
La soluzione vede la combinazioni delle soluzioni viste in precedenza dopo le analisi delle vulnerabilità e si trova pronta a fronteggiare problemi inerenti ad attacchi DDoS ed attacchi Malware limitando danni ed infezioni della rete aziendale.
La configurazione ottimale vede l'ancoraggio della web app ad internet, al di fuori della rete aziendale, cosi da ottenere una schermatura delle informazioni interne, possibile vulnerabilità per attacchi Malware, con l'aggiunta di un Web Application Firewall posizionato tra internet e la web app, che andrà a regolamentare il traffico proteggendo l'e-commerce da possibili attacchi web che comprometterebbero il business aziendale.



Upgrade consigliati

Dopo aver analizzato le varie vulnerabilità della rete aziendale, ci teniamo a consigliare di affrontare gli aggiornamenti adottati nelle soluzioni.

1. Web Application Firewall (WAF)

- AWS Firewall Manager: servizio di gestione centralizzata che consente di configurare e gestire regole di sicurezza, due tipi di piani “Standard” e “Advanced”, possibilità di personalizzare le regole in base alle necessità aziendali. I costi variano in base alle richieste e si basano sul numero di regole, sul numero di account ed i vari extra.
  - Regole a partire da 1$ ca.
  - Abbonamento mensile account AWS Shield Advanced 3000$
- Cloudflare: è una piattaforma di servizi di sicurezza e prestazioni per siti web e applicazioni. Fornisce una vasta gamma di soluzioni per proteggere e accelerare le risorse online, migliorando la sicurezza contro varie minacce online. Offre vari pacchetti di configurazione del WAF, variano in base alle prestazioni ed i costi partono da 20$/mese a 200$/mese, fino al piano personalizzato con costi speciali e specifici.

Nel caso si volesse aggiornare la situazione del firewall attuale possiamo consigliare l’edizione Cisco ASA 5506 - X vista in lavorazioni precedenti a questa.
I costi del firewall variano in base alla configurazione voluta, i singoli device si aggirano intorno ai 550€ ca., mentre la configurazione completa, composta da rack, cablaggi, device e raffreddamento, si aggira intorno ai 2000€.

Thanks.

Contact Us

Marco Malizia | Dataschields
info@datashields.com
datashields.tech