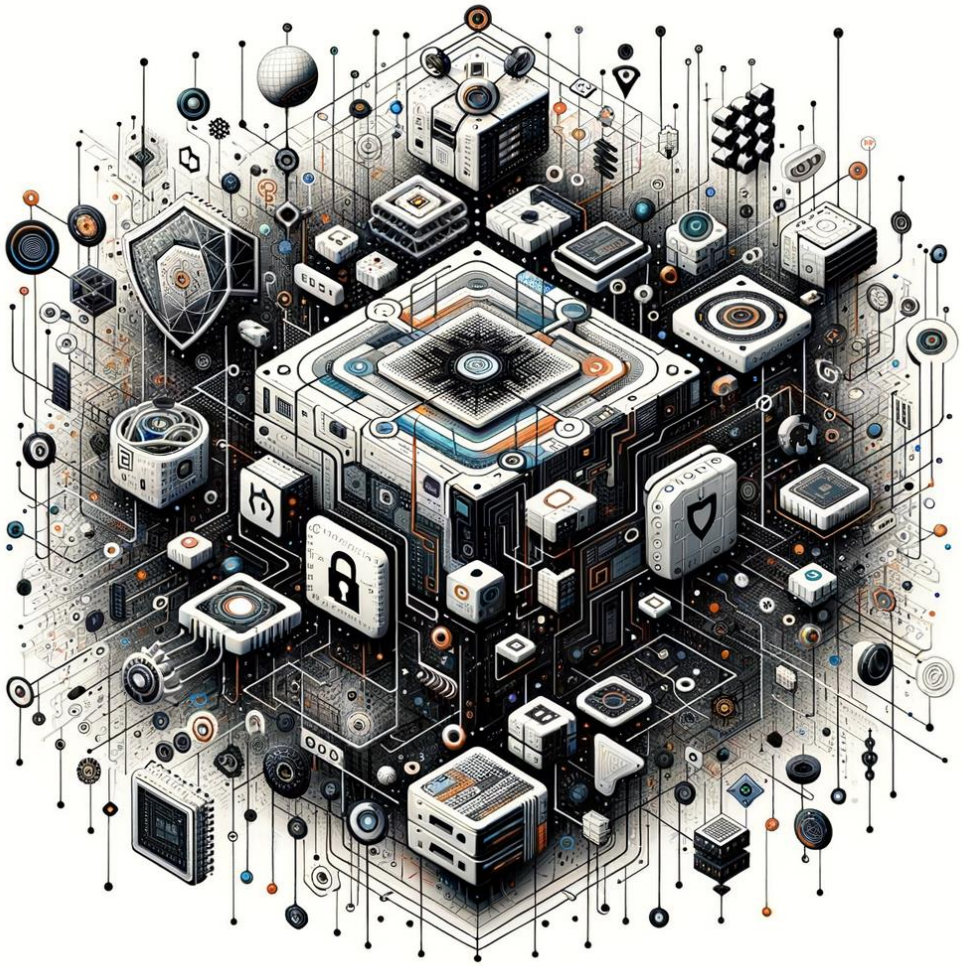
Security Operation

CSPT0324 Modulo 5



Yilei Wu

24 Novembre 2024

Indice

Traccia

Con riferimento alla figura in slide 2, 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 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.

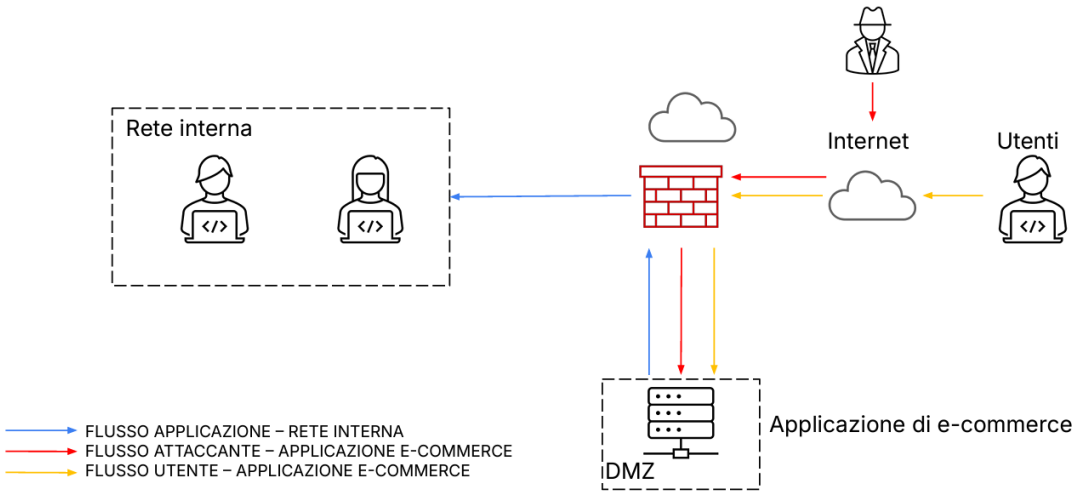
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

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.



Svolgimento

Descrizione dell'architettura di rete iniziale

Dall'architettura data in traccia si rilevano tre macroaree, ciascuna con il proprio flusso:

- **Rete interna aziendale**:
    - Flusso applicazione – rete interna (blu);
- **DMZ – Applicazione e-commerce**;
- **Utenti che accedono dalla rete esterna/internet**, compresi eventuali malintenzionati:
    - Flusso utente – applicazione e-commerce (arancione);
    - Flusso attaccante – applicazione e-commerce (rosso).

Tutte le aree citate sono collegate alla DMZ e i loro flussi sono regolati da un firewall, il quale dovrebbe filtrare la rete interna dai flussi provenienti dalla rete esterna.

La logica di funzionamento è la seguente:

1. L'utente accede al sito dell'e-commerce digitando il relativo dominio/link su internet.
2. Prima di raggiungere l'applicazione di e-commerce, il firewall dell'azienda filtra, riconoscendo l'autore della richiesta come un utente esterno e consente l'accesso alle pagine pubbliche, come il catalogo prodotti, il carrello, l'acquisto, la pagina di login che costituiscono la parte front-end.
3. Dopo che l'utente ha inviato una richiesta e/o effettuato un acquisto, gli utenti della rete interna dell'azienda ricevono le informazioni relative all'ordine, per procedere con l'elaborazione e l'evasione degli ordini. Anche in questo passaggio il flusso di dati che arrivano alla rete interna è filtrato dallo stesso firewall.
4. Anche se le frecce non sono bidirezionali in figura, dalla rete interna dovrebbe partire un segnale di conferma e/o evasione ordine all'applicazione e-commerce e quest'ultima invia una notifica all'utente cliente sullo stato dell'ordine.

Si nota che la rete interna, per comunicare con la rete esterna/internet, lo delega all'applicazione di e-commerce, ovvero, l'interazione tra la rete interna e la rete esterna/internet avviene esclusivamente attraverso l'applicazione e-commerce, senza connessione diretta.

È importante notare che nella rete interna, come indicato nella figura, non segmentata, sono probabilmente presenti non solo i dati del singolo cliente che ha effettuato l'ordine, ma anche informazioni relative ad altri clienti e dati amministrativi, come informazioni sui dipendenti, buste paga, scansioni di documenti, ecc.

Esempio di scenario reale

In uno scenario reale, un'azienda media/ piccola che desidera avviare la vendita online può utilizzare il servizio Shopify, acquistato come pacchetto che include dominio, hosting, bot per le notifiche e caselle email.

In questo caso, il parallelismo sarebbe:

- Rete interna = computer aziendale (es. utilizzo di Danea Easyfatt per ordini, fatture, inventario ecc..)
- Shopify = applicazione di e-commerce

Il servizio Shopify viene sincronizzato con il computer aziendale, consentendo l'elaborazione interna degli ordini ricevuti sulla piattaforma di e-commerce.

Si cita Shopify solo a titolo esemplificativo, poiché esistono molte altre soluzioni, come WooCommerce, Wix, PrestaShop e molti altri.

Scenario 1 – Azioni Preventive

Exploit oggetto di analisi

Il **Cross-Site Scripting** è un attacco in cui un malintenzionato inserisce script dannosi in pagine web visitate da altri utenti. Sono principalmente causate da un input utente che non viene correttamente "sanitizzato" o controllato prima di essere gestito da una data applicazione web.

La **SQL Injection** è un tipo di attacco che sfrutta le debolezze nei sistemi che utilizzano i database. Permette a un malintenzionato di inviare comandi dannosi al database di un sito web.

Soluzioni

- **Sanitizzare gli input e output intervenendo sul codice**: è la misura più efficace poiché affronta direttamente la vulnerabilità. Tuttavia, in situazioni reali, modificare il codice esistente potrebbe non essere sempre fattibile a causa di risorse limitate o applicazioni legacy.
- **Adottare un Web Application Firewall (WAF)**: è un'ottima soluzione complementare. Un WAF è un sistema di sicurezza che protegge le applicazioni web monitorando e bloccando il traffico malevolo. Un esempio di servizio molto conosciuto è Cloudflare (famoso tra i utenti privati per il servizio DNS).
- **IPS (Intrusion Prevention System)**: è un sistema di prevenzione che rileva e può anche bloccare attivamente le minacce in tempo reale, operando in modo automatico.

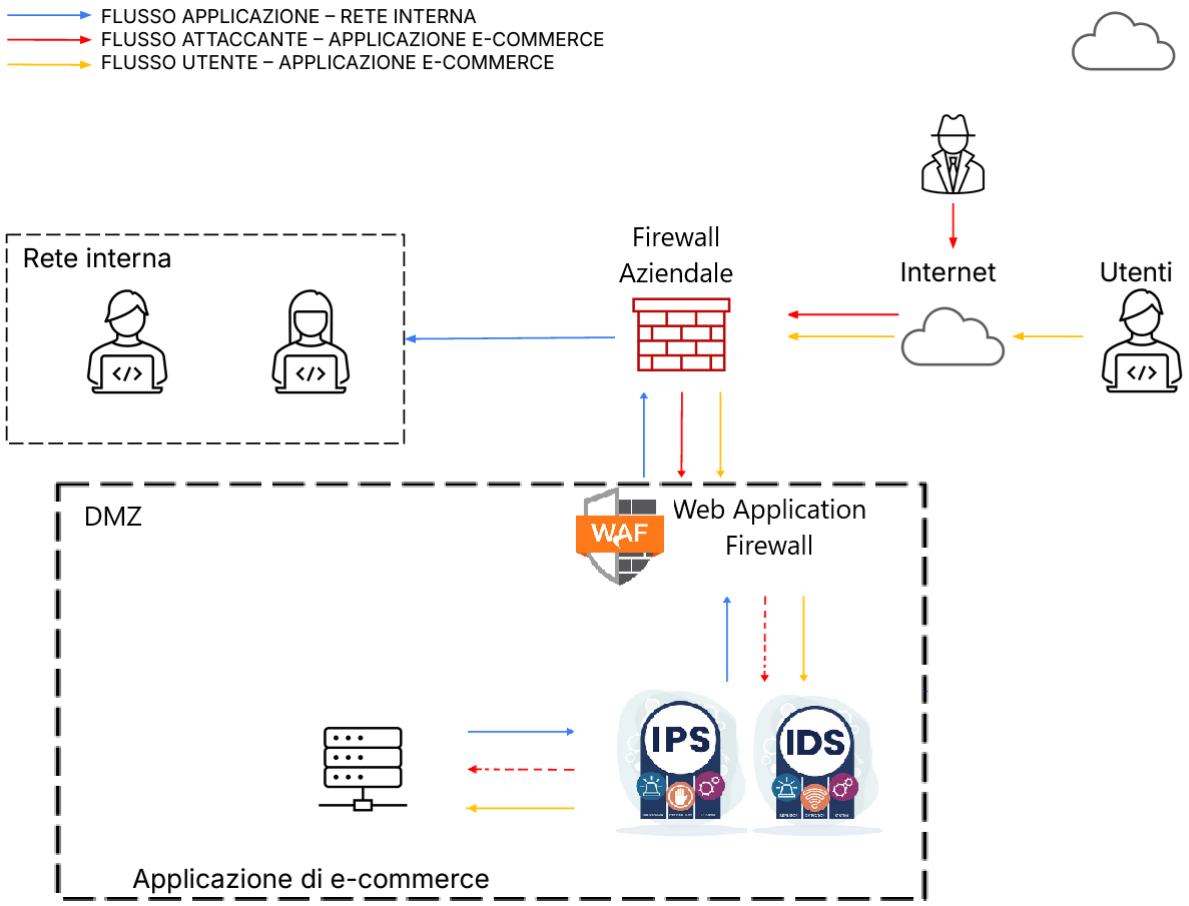
La soluzione migliore è un approccio ibrido che combina tutte le strategie sopra citate. Infatti, mentre il WAF e l'IPS non risolvono le vulnerabilità nel codice, sorvegliano il traffico in ingresso e in uscita.

Un'analogia utile è quella di una casa con una porta rotta (la vulnerabilità): se si mette una super guardia (WAF/IPS) a controllare chi entra e esce, tuttavia la porta rimane rotta. La soluzione ideale sarebbe riparare la porta (remediation) e mantenere la super guardia per garantire una protezione aggiuntiva.

Esiste un'alternativa all'IPS, che è l'IDS (Intrusion Detection System). Tuttavia, l'IDS si limita a rilevare le minacce senza bloccarle, e quindi ha un costo inferiore.

È importante considerare che l'implementazione di questi sistemi comporta dei costi; per questo, è fondamentale che un'azienda valuti il budget disponibile per implementare le proprie misure di sicurezza.

Architettura di rete integrata di un WAF e un IPS o IDS



Commento

Quando un utente, sia legittimo che malintenzionato, si connette all'applicazione di e-commerce dall'esterno attraverso Internet, il suo traffico passa prima attraverso il firewall aziendale. All'interno della DMZ, questo traffico viene filtrato e ispezionato dal Web Application Firewall (WAF) prima di raggiungere l'applicazione di e-commerce.

Mentre l'utente è connesso all'applicazione, la sua attività viene monitorata in tempo reale dal sistema IPS (Intrusion Prevention System) o IDS (Intrusion Detection System), posizionato tra il WAF nella DMZ e l'applicazione di e-commerce. Quando vengono rilevati comportamenti sospetti o attività malevole, con l'IPS, può intervenire attivamente per bloccare tali tentativi di intrusione, mentre con l'IDS viene solamente rilevato e notificato.

Se si ipotizza invece che il codice relativo agli input/output fossero stati sanitizzati, questa vulnerabilità sarebbe rimediata e quindi la superficie d'attacco è ridotta. Tuttavia è consigliabile ugualmente il mantenimento della WAF e del IPS/IDS.

Solo il traffico che supera i controlli di sicurezza del firewall aziendale, del WAF nella DMZ e del sistema IPS/IDS viene infine autorizzato ad accedere all'applicazione di e-commerce. Questa applicazione a sua volta trasmette il flusso di dati all'interno della rete interna dell'azienda.

La DMZ si interpone quindi tra la rete interna ed esterna/Internet.

Le frecce in rosso rappresentante il flusso dell'attacante nella DMZ sono tratteggiate per le implementazioni adottate e pertanto il rischio di un attacco portato a termine è minore.

Scenario 2 – Impatti sul business

DDos

Un attacco DDoS (Distributed Denial of Service) è quando molte persone o computer, controllati da un attaccante, inviano un numero enorme di richieste a un sito web o a un servizio online. L'obiettivo è sovraccaricare il server che gestisce il sito, impedendo così che possa rispondere alle richieste legittime. Uno degli episodi più famosi sono stati una serie di attacchi DDoS da parte degli attivisti Anonymous ai siti istituzionali americani a seguito della chiusura di Megaupload nel 19 gennaio 2012.

Calcolo danni stimati

Tempo fuori servizio (Tfs)	Vendita media al minuto (VmM)	Danni lordi totali (prodotto Tfs*VmM)
10	**€ 1.500,00**	**€ 15.000,00**

Si prega di notare che questi dati sono grezzi e non tengono conto degli aspetti fiscali relativi al danno, poiché non si conosce lo stato e regime fiscale in cui opera l'azienda. Alcuni punti da considerare:

- Le imposte a carico del cliente finale, in questo caso l'e-commerce, possono includere l'applicazione di aliquote IVA.
- Contabilmente la minor vendita, come mancato guadagno, non può essere registrata come perdita, poiché è solo ipotetica. Infatti devono derivare da eventi concreti e misurabili. In questo caso, il calcolo dei danni rappresenta una stima della potenziale perdita.
- Non si sono tenuti conto invece dei costi relativi per il ripristino dell'attività di business.

Soluzioni

Filtraggio e monitoraggio del Traffico

Firewall, WAF e IDS/IPS: questi strumenti, come citato nel scenario 1, sono fondamentali per la sicurezza della rete. Filtrano automaticamente il traffico, bloccando richieste malevole. L'efficacia di questi strumenti dipende dalla loro configurazione e dalla competenza di chi li gestisce.

SIEM (Security Information and Event Management): raccoglie e analizza dati di sicurezza per identificare minacce e anomalie. Fornisce una visione centralizzata degli eventi di sicurezza, facilitando l'individuazione di comportamenti sospetti.

SOAR (Security Orchestration, Automation, and Response): è un sistema software avanzato che svolge un ruolo fondamentale nella gestione e automazione della risposta agli incidenti di sicurezza informatica intervenendo direttamente sulle minacce e può essere configurato per funzionare in collaborazione con il SIEM.

Rate Limiting: limita il numero di richieste che un singolo utente o indirizzo IP può inviare in un determinato periodo di tempo. Se un utente supera questa soglia, viene bloccato temporaneamente. Questa misura è utile per prevenire sovraccarichi causati da attacchi automatizzati.

Blocco di IP Sospetti: consiste nel riconoscere e bloccare indirizzi IP che mostrano comportamenti sospetti o che utilizzano VPN e proxy. Questa strategia riduce il numero di potenziali attaccanti e contribuisce a mantenere la sicurezza del sistema.

Sistemi di Mitigazione DDoS: servizi offerti come Cloudflare e Amazon Shield offrono protezione specifica contro attacchi DDoS. Questi sistemi filtrano il traffico dannoso prima che raggiunga il server, garantendo la continuità del servizio. Le aziende che forniscono tali servizi sono generalmente grandi e specializzate, offrendo un alto grado di affidabilità.

CAPTCHA e Verifiche Umane

Dimostra di essere un umano: quando un utente fa molte richieste in poco tempo, viene chiesto di completare un CAPTCHA (un test semplice, come identificare immagini, ascoltare audio ecc…). Questo aiuta a distinguere tra umani e bot automatici, riducendo il carico sul server.

Utilizzo di CDN (Content Delivery Network)

Le **CDN** sono progettate per distribuire il traffico su più server situati in diverse posizioni geografiche. Questo richiede che l'azienda disponga di più server, il che porta a diversi vantaggi:

- **Velocità di Caricamento**: gli utenti possono accedere ai dati dal server più vicino a loro, riducendo significativamente il tempo di caricamento del sito.
- **Gestione del Traffico**: durante attacchi DDoS, le CDN assorbono il traffico in eccesso, distribuendo il carico tra i vari server. Questo consente di mantenere il sito operativo anche in situazioni di alta pressione.
- **Affidabilità**: se un server si guasta, gli utenti possono comunque accedere al contenuto tramite un altro server della rete, garantendo così una continuità del servizio.

Questa soluzione rispecchia perfettamente uno dei principi più apprezzato dagli ingegneri: la ridondanza.

Resilienza

Disaster Recovery as a Service (DRaaS): implementare una soluzione DRaaS consente di attivare rapidamente un'infrastruttura cloud o secondaria in caso di attacco o disastro. Questo approccio facilita il ripristino del servizio in tempi brevi e garantisce che il sistema rimanga operativo fino al completo recupero dei server compromessi tale da minimizzare il downtime e mantenere la continuità operativa, assicurando che i dati siano protetti e che i servizi siano nuovamente disponibili il prima possibile.

Commento

Tutte queste soluzioni comportano costi variabili. È essenziale che l'azienda valuti attentamente rischi e benefici, considerando cosa proteggere e se l'investimento è giustificato. In particolare, dovrebbero essere presi in considerazione:

- **Maximum Tolerable Downtime (MTD)**: il tempo massimo in cui un sistema può rimanere inattivo senza gravi conseguenze.
- **Recovery Time Objective (RTO)**: il tempo necessario per ripristinare i servizi dopo un'interruzione.
- **Annualized Rate of Occurrence (ARO)**: la frequenza prevista di attacchi o eventi avversi in un anno.

La perdita di 15.000 euro in 10 minuti rappresenta un danno contenuto per questa azienda che, a calcoli stimati, fattura 2.160.000 euro al giorno (circa 800 milioni di euro all'anno). Ciò implica che l'azienda in questione è paragonabile alle più grandi e conosciute aziende di e-commerce nel mondo, come:

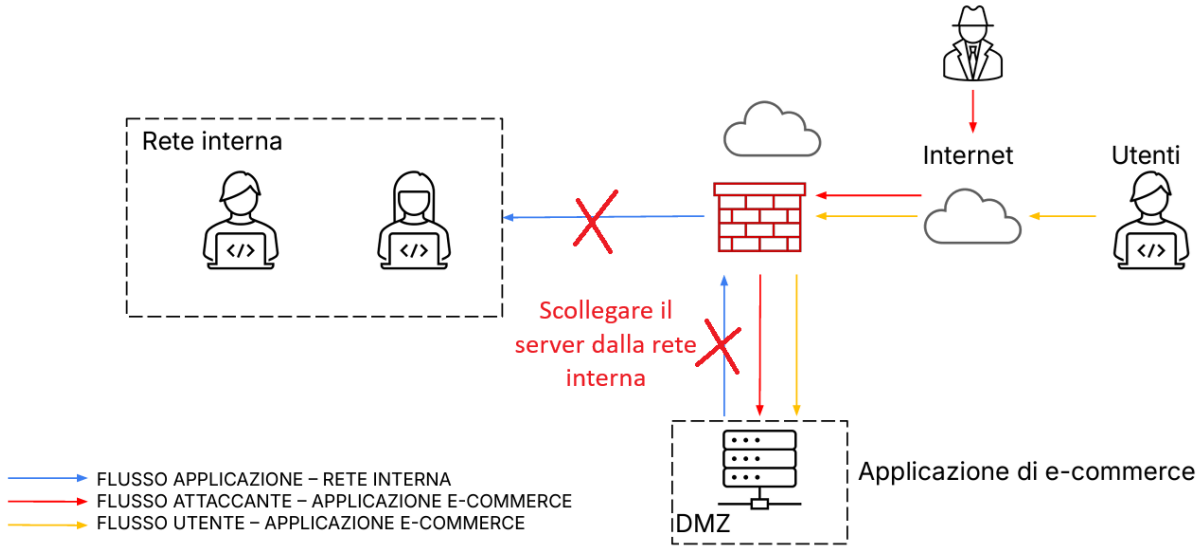
- **Amazon**: Leader globale dell'e-commerce, con vendite che superano i miliardi di euro ogni giorno.
- **Alibaba**: Gigante dell'e-commerce in Cina, gestisce piattaforme come Taobao e Tmall, con volumi di vendita enormi.
- **Walmart**: Ha una forte presenza online che contribuisce a generare elevate entrate quotidiane.
- **eBay**: Una delle prime piattaforme di e-commerce, continua a generare fatturati consistenti.
- **JD.com**: Un altro grande player cinese con un modello di business solido e vendite elevate.

Pertanto, per un'azienda di tali dimensioni, tutte le soluzioni proposte e le più moderne in fase di sviluppo non citate e non affrontate da questo corso, sono fortemente consigliate, poiché i potenziali danni sarebbero ancora maggiori in caso di attacco.

Scenario 3 – Response

Evitare la propagazione del Malware

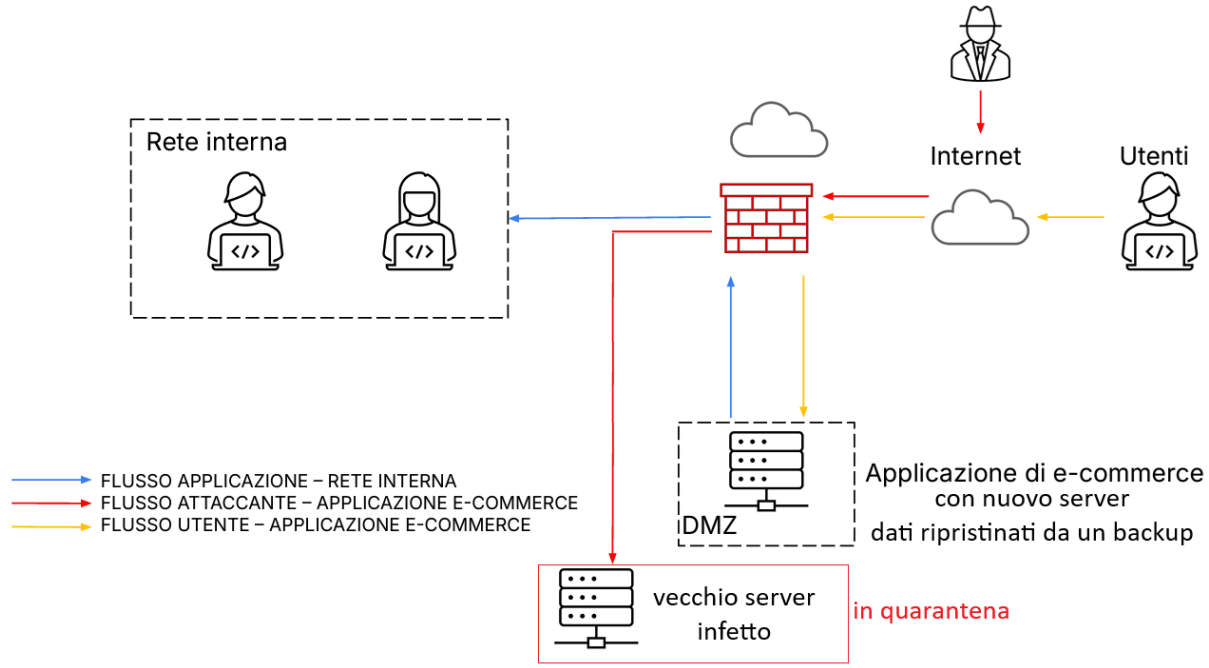
Per evitare la propagazione del malware che ha infettato il server dell'applicazione di e-commerce, l'azione prioritaria è scollegarla dalla rete interna, in questo modo non potrà propagarsi su altre macchine dell'azienda.



Conseguenze

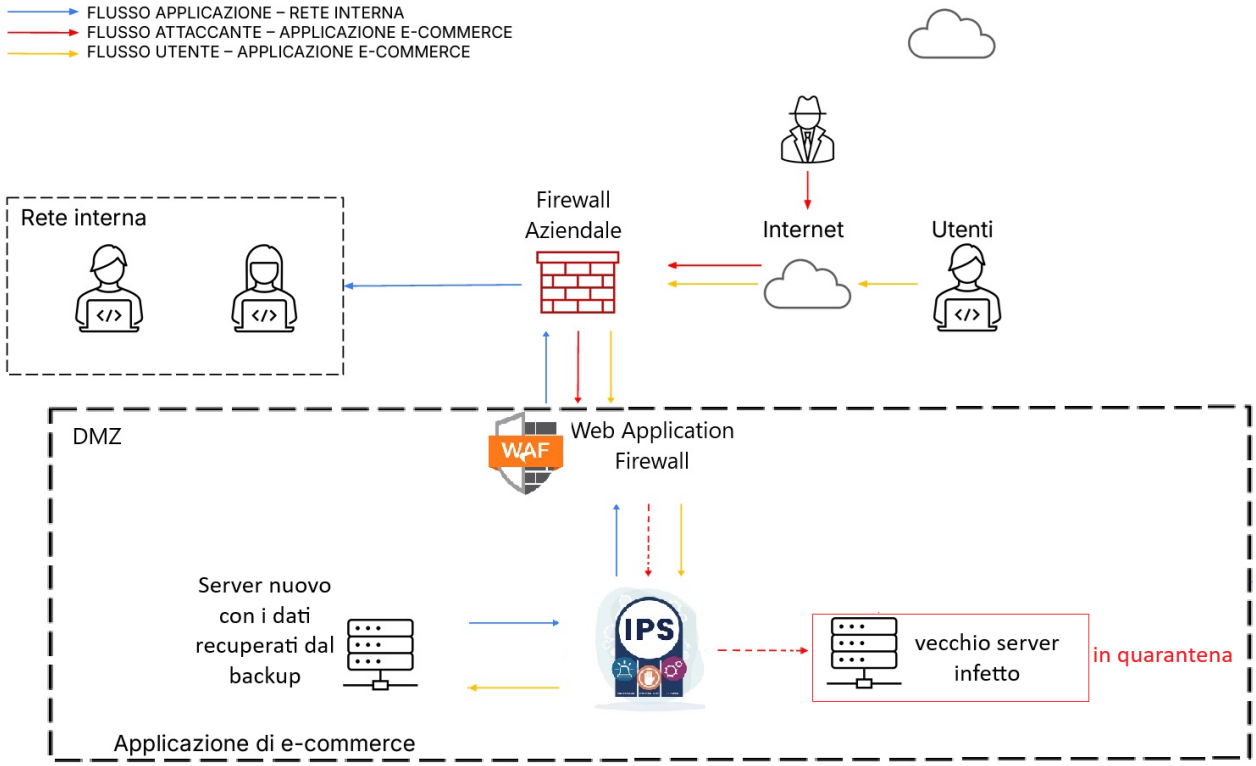
In uno scenario senza adeguate misure di continuità operativa e disaster recovery, avendo un unico server nella DMZ compromesso, l'interruzione completa del servizio e-commerce sarebbe inevitabile. Il tempo di ripristino (RTO) rischierebbe di essere inaccettabilmente lungo, con gravi conseguenze disastrose per l'attività di business.

Implementazione immediata ed efficace



In questo scenario, i backup quotidiani hanno permesso di sostituire il server infetto con uno nuovo, ripristinando la continuità operativa e mettendo in quarantena il server compromesso, impedendone la propagazione e quindi ulteriori danni. Tuttavia, l'accesso dell'attaccante al server infetto non è stato ancora rimosso.

Scenario 4 – Soluzione completa



Si sono integrate le soluzioni dello scenario 1 con le soluzioni dello scenario 3. L'architettura di rete è più sicura con la presenza di

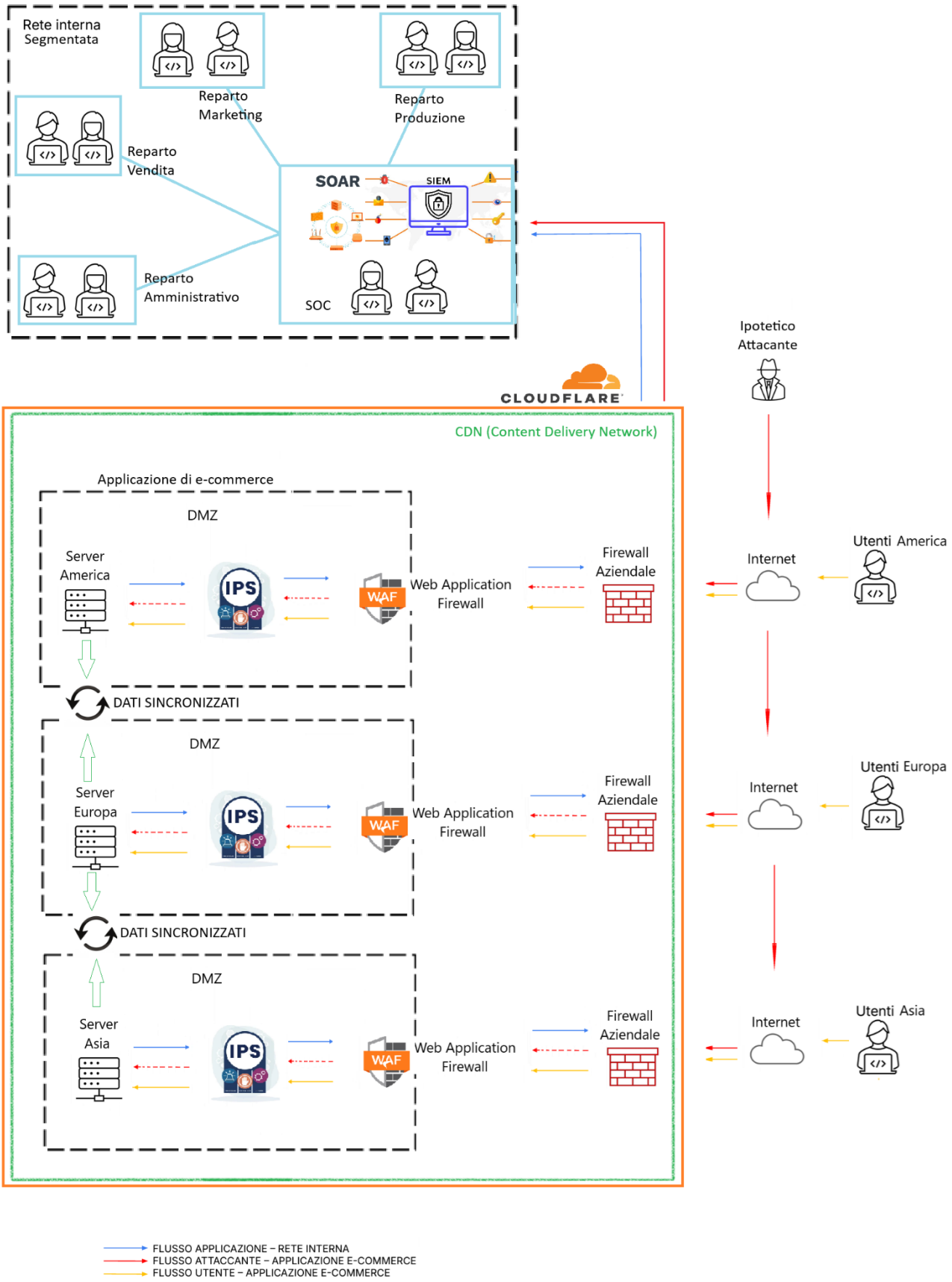
- Firewall Aziendale
- Web Application Firewall
- IPS
- Backup quotidiano
- Isolamento del server infetto

Tuttavia come già affermato nel paragrafo del commento Scenario 2, l'azienda ha un elevato volume d'affari e non, deve e può, accettare un'architettura simile, che probabilmente è più adatto per piccole medie imprese.

Nel prossimo paragrafo, Scenario 5, si illustra un'architettura di rete più adeguata.

Scenario 5 – Modifica dell'infrastruttura

Grafico architettura di rete



Commento – protezione multilivello

Questa architettura di rete presenta diverse caratteristiche fondamentali per garantire la sicurezza e la continuità del servizio di e-commerce.
Sono state introdotte le soluzioni descritte nel paragrafo relativo allo scenario 2.

Ridondanza e bilanciamento del carico

L'applicazione di e-commerce è distribuita su tre server, con i dati sincronizzati tra di loro. Un servizio di Content Delivery Network (CDN), come Cloudflare o Microsoft Azure, gestisce il traffico in entrata, indirizzando gli utenti al server più vicino in base alla loro posizione geografica (America, Europa, Asia). Questo approccio migliora non solo l'efficienza e la velocità del servizio, ma aiuta anche a prevenire interruzioni in caso di guasti o attacchi.

Firewall

Il firewall aziendale svolge diverse funzioni di sicurezza, tra cui:

- Bloccare gli indirizzi IP sospetti.
- Limitare il numero di richieste da singoli utenti o indirizzi IP.
- Utilizzare un servizio esterno per mitigare gli attacchi DDoS (come Cloudflare in figura).
- Implementare sistemi CAPTCHA per distinguere tra utenti umani e bloccare utenti bot.

Protezione DMZ

Nella zona demilitarizzata (DMZ) sono presenti:

- Un Web Application Firewall (WAF) che filtra e ispeziona il traffico in entrata.
- Un Intrusion Prevention System (IPS) che monitora e blocca attivamente gli attacchi.

Soc

Il Security Operations Center (SOC) è un dipartimento essenziale per garantire la sicurezza di un'azienda. Si occupa di monitorare, analizzare e rispondere a potenziali problemi di sicurezza, utilizzando un sistema SIEM per raccogliere informazioni da diverse fonti e identificare rapidamente anomalie o attacchi.
All'interno del SOC, c'è il SOAR che è un sistema software avanzato che coordina e automatizza la risposta agli incidenti di sicurezza. Quando il SIEM rileva una minaccia, il SOAR può intervenire in maniera diretta, avviando procedure standardizzate di mitigazione, come l'isolamento di sistemi compromessi o l'aggiornamento di firewall. Questa automazione della risposta permette di accelerare notevolmente i tempi di reazione e ridurre l'impatto degli attacchi.

Segmentazione della rete

La segmentazione della rete interna divide l'infrastruttura in aree separate. Questo limita la diffusione di eventuali incidenti a una sola parte della rete, evitando che si propaghino in altri reparti. Inoltre, consente di applicare controlli di accesso più mirati per proteggere meglio le zone più critiche.

Miglioramento continuo della sicurezza e formazione del personale

Per mantenere un livello di sicurezza eccellente, l'azienda non deve limitarsi solamente agli aspetti tecnici come aggiornamenti, valutazioni delle vulnerabilità e test di penetrazione a cadenza regolare. È altrettanto cruciale investire nella formazione continua del personale in ambito di sicurezza informatica, inclusi i rischi di social engineering.

Conclusione

Nonostante queste misure, se un attaccante riesce a infiltrarsi nella rete interna, il SOC interviene per bloccare e isolare il computer infetto, riducendo al minimo i danni.
È importante notare che questa architettura richiede un investimento significativo, il che potrebbe renderla inaccessibile per alcune aziende, in particolare quelle di dimensioni più piccole o con budget limitati. Tuttavia, per aziende con un volume d'affari multimilionario, questo investimento è fondamentale per garantire la sicurezza.