



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 vostra 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)

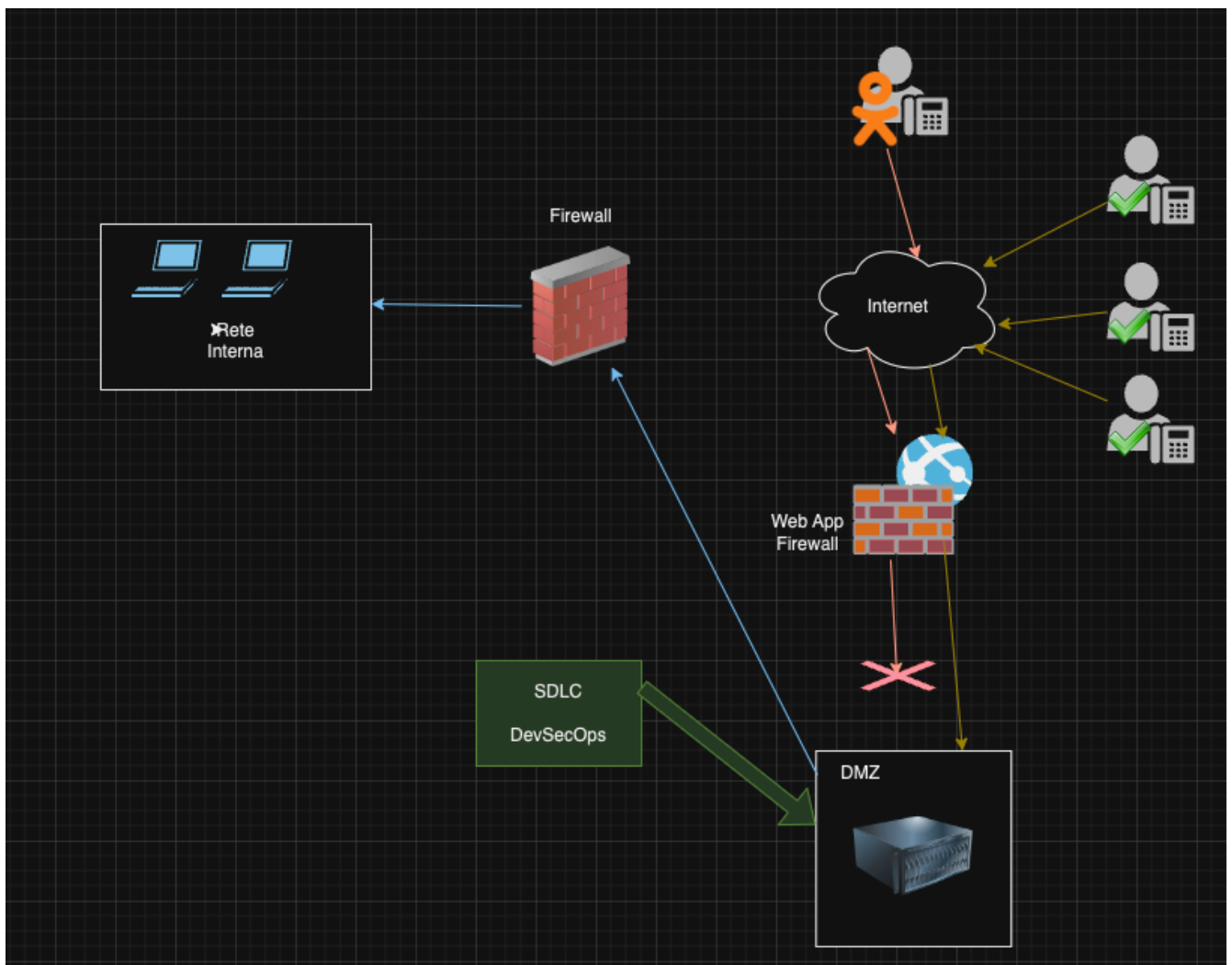
Svolgimento:

Svolgimento del punto numero 1

Nel punto numero 1 ci viene chiesto di concentrarci su azioni preventive per difendere l'applicazione web.

Modifica delle rete con aggiunta di uno WAF (Web Application Firewall) con funzioni di sicurezza dedicate alla protezione di applicazioni web da attacchi SQL Injection e Cross Site Scripting (XSS).

Sanitizzazione del software con aggiunta di un modello SDLC a scelta tra quello a “ spirale “ oppure quello “ agile “ , integrazione del modello DevSecOps per integrare test di sicurezza in ogni fase del modello precedente.

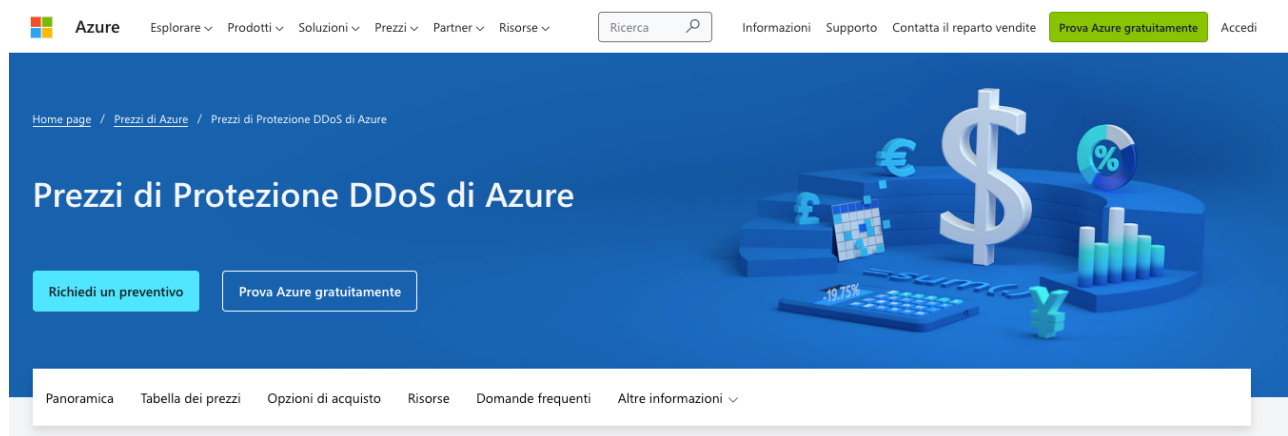


Svolgimento del punto numero 2

Nel punto numero 2 abbiamo un attacco di tipo DDos che ferma la nostra applicazione per un tempo di 10 minuti con un impatto di 1.500 €/minuto.

Possiamo calcolare la perdita data dal singolo evento pari ad € 15.000 ma non possiamo determinare una stima sulla perdita annua dato che non sappiamo quante volte si può sviluppare l'evento.

Decidiamo in accordo con i dirigenti di investire in una soluzione che ci protegge dagli attacchi DDoS



La soluzione presenta un costo di \$ 2.944/mese quindi la scommessa dell'azienda è che dopo i primi 30 minuti di negazione del servizio saremo in guadagno.

Data la plausibilità di n attacchi durante l'anno optiamo per questo tipo di DRaaS (Disaster Recovery as a Service)

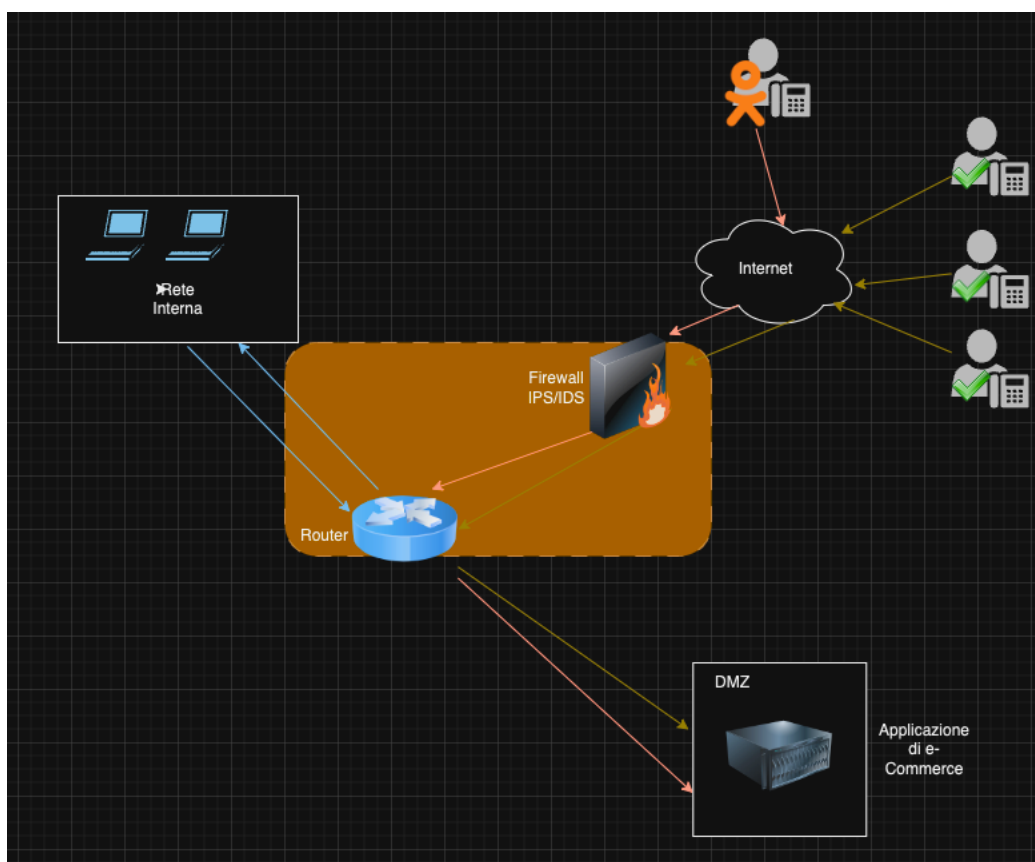
	Prezzo
Addebito mensile (inclusa la protezione per 100 risorse indirizzo IP pubblico)	\$2.944/mese

Svolgimento punto numero 3

In questo punto non ci concentriamo sulla rimozione del malware che ha infettato la nostra applicazione bensì sulla sua non propagazione verso la nostra rete interna.

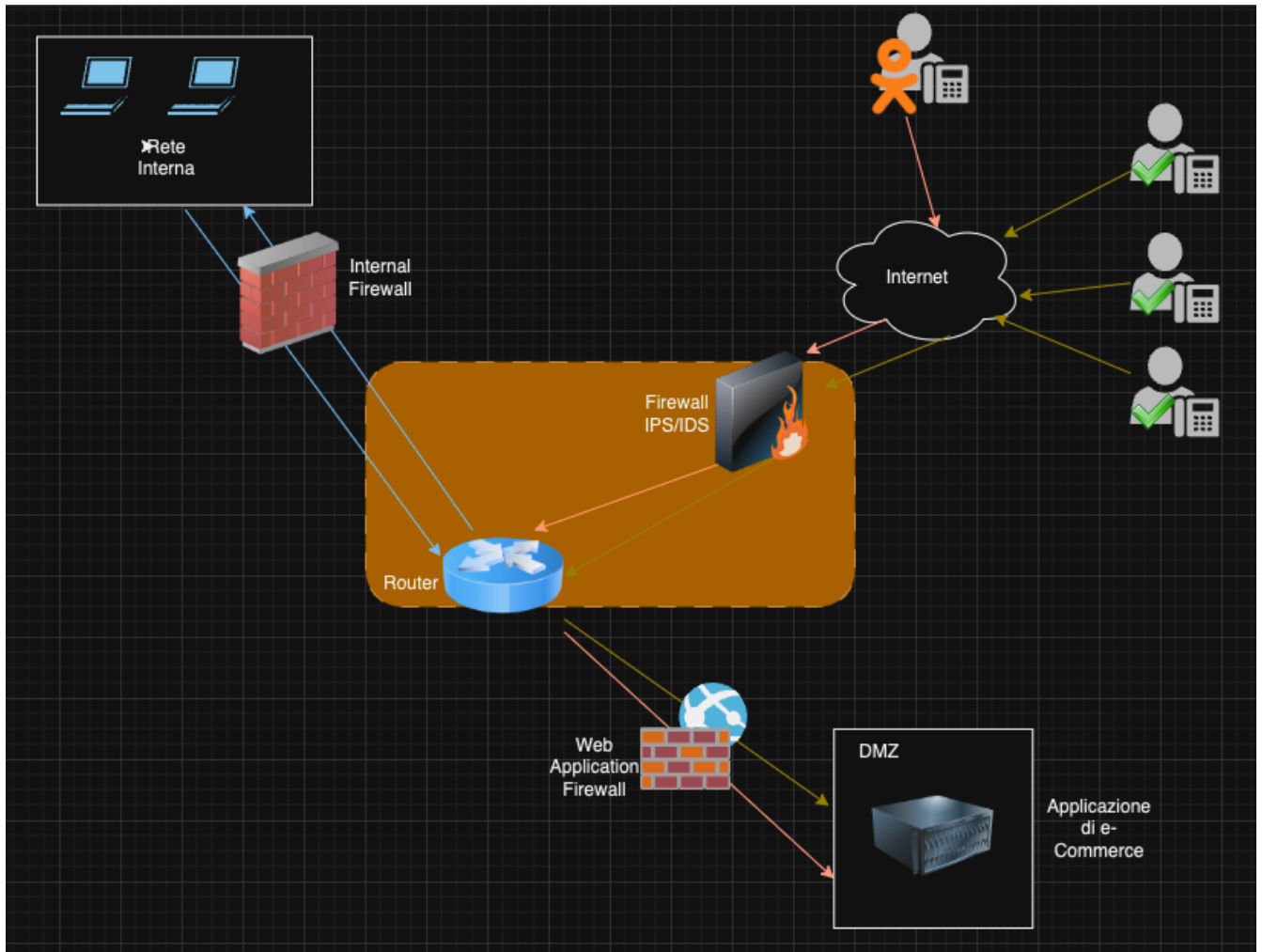
Per fare questo dobbiamo implementare una soluzione di isolamento dell'incidente e mettiamo di conseguenza in atto una configurazione di segmentazione preventiva della rete.

A valle del nostro firewall andiamo a posizionare un dispositivo di routing (oppure utilizziamo una soluzione che gestisce entrambi i compiti) in modo tale che le due strutture trovino su sottoreti differenti



Svolgimento punto numero 4

Nel punto numero 4 uniamo le soluzioni del punto numero 1 e del punto numero 3 costruendo una rete un po' più strutturata



Svolgimento del punto numero 5

Il punto 5 richiede una modifica più aggressiva dell'infrastruttura. Andiamo quindi ad eseguire una vera e propria riprogettazione della network solution.

Premesse :

. viene svolta una ricerca su google per capire che ordine di grandezza è quello della nostra società

Amazon e Apple irraggiungibili, seguono Google e Microsoft: le cifre

Dopo questa piccola premessa, vediamo realmente quanto fatturano queste aziende in un solo minuto di attività. Al **primo posto** c'è indiscussamente **Amazon**, la società di e-commerce più famosa al mondo movimentata **955.517 dollari al minuto**, praticamente un milione ogni 60 secondi. Il mercato più importante e redditizio per la società di Jeff Bezos rimane quello statunitense, ma nel 2020 l'azienda ha fatturato 49 miliardi di dollari sommando Germania e Giappone.

Al **secondo posto** troviamo **Apple**, la società di elettronica di consumo più conosciuta sul pianeta. Il colosso con sede a Cupertino fattura ben **848.090 dollari al minuto**. Apple è la società tecnologica con la capitalizzazione di mercato più alta al mondo, parliamo di **2.000 miliardi di dollari**.

Conclude il podio **Alphabet**, casa madre di **Google**. La holding del motore di ricerca più usato sul web si ferma a **433.014 dollari al minuto**. Come si può vedere, nonostante siano cifre da capogiro, il distacco tra Alphabet e le prime due classificate è netto. Alphabet ha chiuso il 2020 con un fatturato di 182 miliardi di dollari.

Quarto posto per **Microsoft**, l'azienda fondata da Bill Gates e guidata da Satya Nadella fattura **327.823 dollari ogni 60 secondi**. Anche se fuori dal podio, Microsoft è seconda solo ad Apple per capitalizzazione.

Quinto posto della classifica per **Facebook**, società madre di WhatsApp e Instagram tra e altre. Il colosso capitanato da Mark Zuckerberg ha toccato **213.628 dollari al minuto**. Il primo trimestre del 2021 è stato il migliore nella storia di Facebook con una media di **2,8 miliardi di utenti attivi mensili** sul social network.

Tesla e Netflix si piazzano rispettivamente al **sesto e settimo posto** della lista. L'azienda di Elon Musk fattura **81.766 dollari al minuto**, mentre il gigante dello streaming **50.566 dollari** grazie ai suoi 203 milioni di abbonati.

Capiamo quindi che si tratta di una realtà importante (1.500 € minuto) ma comunque di una realtà di medio piccole dimensioni rispetto ai maggiori attori del mercato.

. trattandosi di una soluzione e-commerce possiamo capire che non abbiamo una realtà che tratta dati a livello di riservatezza paragonabili a segreti militari, segreti governativi, brevetti ecc..

Viste le premesse riprogettiamo l'infrastruttura eseguendo uno “ **spostamento del rischio** ” con l'azione specifica di “ **migrazione verso il cloud** ” della parte di rete che espone il servizio di e-Commerce.

Troviamo quindi un'infrastruttura di rete privata dove la software house gestisce tutti i compiti strettamente relativi alla creazione / mantenimento del business, come ad esempio il rapporto con clienti e fornitori, le modifiche al software ed i miglioramenti allo stesso ecc...

La parte di erogazione del servizio, gestione del rischio, messa in sicurezza la spostiamo al fornitore al quale ci siamo appoggiati per la migrazione verso il cloud (AWS , Microsoft)

Il fornitore del servizio provvederà anche bimestralmente ad eseguire le operazioni di valutazione della sicurezza, che ci costringeranno ad eventuali patching mantenendo lo standard del nostro prodotto in continuo miglioramento.

Esempi di strumenti messi a disposizione dal cloud per il nostro e-commerce

Prezzi di Database di Azure per MySQL

D64ds v4	64	256 GiB	€4.789,145/mese	€2.871,3334/mese ~40% di risparmio	€1.915,6579/mese ~60% di risparmio
----------	----	---------	-----------------	---------------------------------------	---------------------------------------

Prezzi di App Center

Piano di test Standard	Esegui test dell'interfaccia utente su migliaia di dispositivi reali e di configurazioni del sistema operativo.	La concorrenza di ogni dispositivo include 30 ore dispositivo.	€91,262/mese concorrenza per compilazione
------------------------	---	--	--

