Rafael Mango

Report progetto

CYBER SECURITY & ETHICAL HACKING

Indice

indice 1

traccia 2

azioni preventive 3

Impatti sul business 4

Response 5

Soluzione completa 6

Modifica «più aggressiva» dell'infrastruttura 7

Ringraziamenti 8

Traccia

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

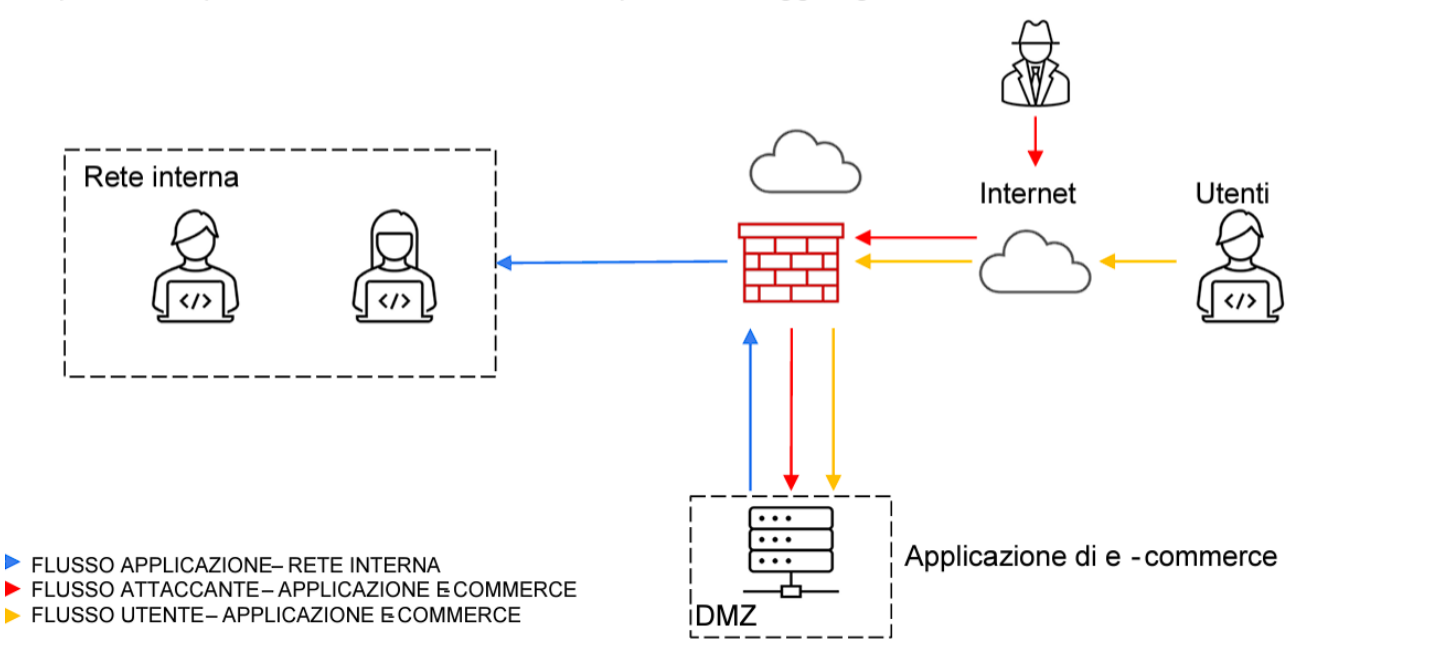
1.Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo DDoSdall'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 malwarenon 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: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2 .



Risposte quesiti

1-Azioni preventive :

-Per difendere l'applicazione Web da attacchi di tipo SQLi (Injection SQL) o XSS (Cross-Site Scripting) da parte di un utente malintenzionato, è possibile implementare diverse azioni preventive come:

-Validazione dei dati di input: Assicurarsi che tutti i dati inseriti dagli utenti attraverso form o altri mezzi siano correttamente validati prima di essere utilizzati dal sistema. Questo può prevenire gli attacchi SQLi e XSS.

-Utilizzo di prepared statements e parametrizzazione delle query SQL: Evitare la concatenazione di stringhe per creare query SQL dinamiche. Invece, utilizzare prepared statements

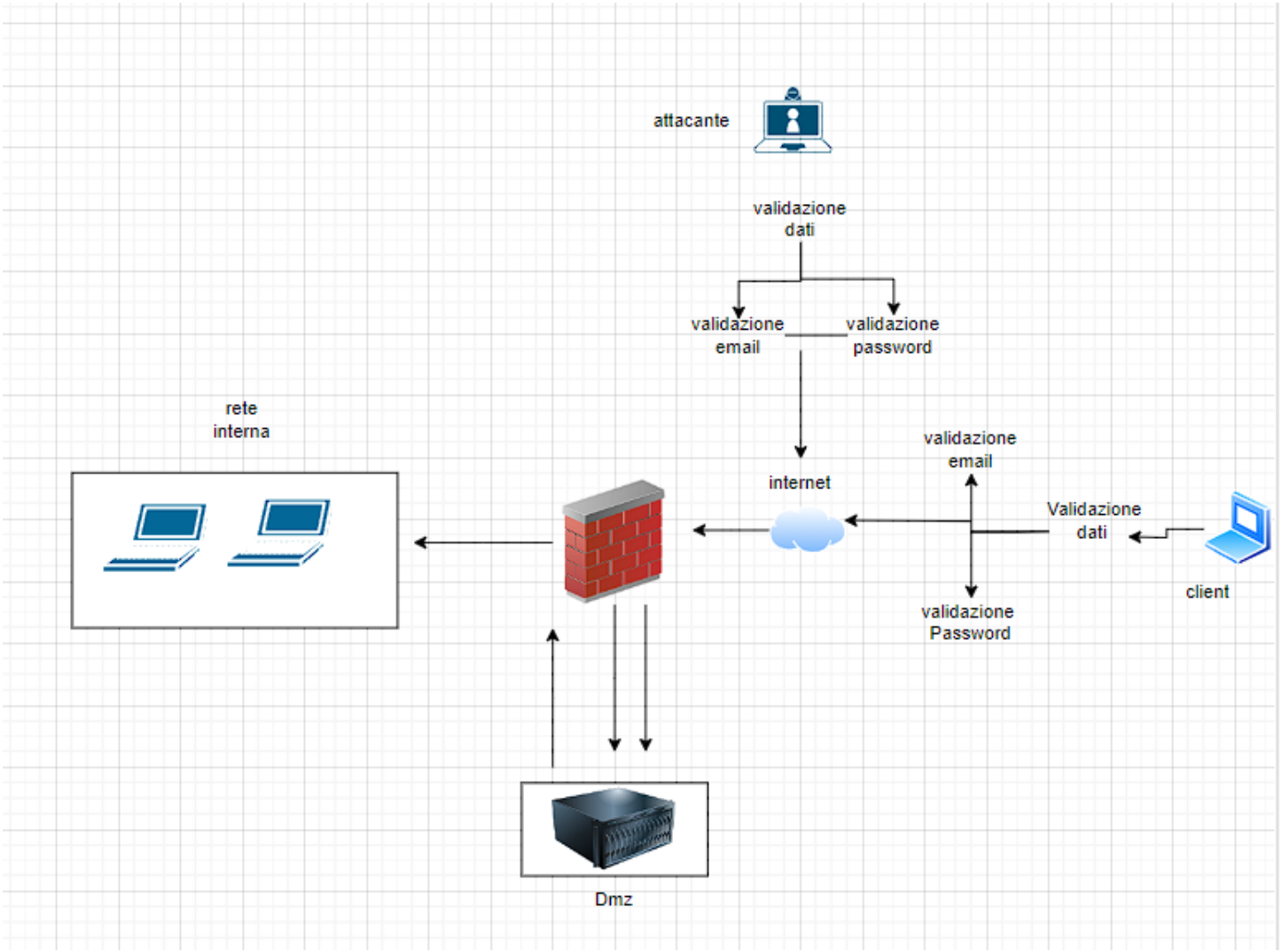
e parametrizzazione dei parametri per garantire che i dati inseriti dagli utenti non possano essere interpretati come parte della query SQL.

-Sanitizzazione degli input: Pulire e filtrare i dati di input dagli utenti per rimuovere caratteri speciali e codice potenzialmente dannoso. Questo può prevenire gli attacchi XSS.

-Utilizzo di framework e librerie sicure: Utilizzare framework e librerie web che offrono protezione incorporata contro attacchi comuni come SQLi e XSS. Queste soluzioni spesso includono funzionalità di validazione e sanificazione dei dati automatiche.

-Implementazione di policy di sicurezza: Stabilire e far rispettare rigorose policy di sicurezza per lo sviluppo e la manutenzione dell'applicazione, compresi processi di revisione del codice e test di sicurezza regolari.

esempio di validazione dei dati .



che cosa è attacco di tipo SQLi e XSS:

SQL Injection (SQLi):

- SQL injection è un tipo di attacco informatico in cui un attaccante inserisce codice SQL malevolo all'interno di campi di input di un'applicazione web. Questo codice SQL dannoso viene poi eseguito dal database backend dell'applicazione quando elabora la richiesta dell'utente.
- L'obiettivo principale di un attacco SQL injection è quello di manipolare le query SQL dell'applicazione per ottenere l'accesso non autorizzato ai dati sensibili presenti nel database o per eseguire operazioni dannose come l'eliminazione o la modifica dei dati.

Cross-Site Scripting (XSS):

- Cross-site scripting è un tipo di vulnerabilità web che consente agli attaccanti di iniettare script malevoli (solitamente JavaScript) all'interno delle pagine web visualizzate dagli utenti. Questi script possono essere eseguiti sul browser degli utenti vittima, consentendo all'attaccante di rubare informazioni sensibili, interagire con l'interfaccia utente, reindirizzare gli utenti verso siti dannosi e molto altro ancora.
- Gli attacchi XSS possono essere suddivisi in tre categorie: stored (salvati), reflected (riflessi) e DOM-based (basati sul DOM), a seconda di come il payload malevolo viene fornito e eseguito.

Entrambi gli attacchi rappresentano gravi minacce per la sicurezza delle applicazioni web e possono portare a violazioni dei dati, danni alla reputazione, perdite finanziarie e molto altro ancora se non trattati correttamente.

---

2. Impatti sul business

Per calcolare l'impatto finanziario dell'attacco DDoS, possiamo moltiplicare il valore medio delle transazioni degli utenti per il tempo di inattività del servizio.

Dato che gli utenti spendono in media 1.500 € al minuto sulla piattaforma di e-commerce e il servizio è stato reso non raggiungibile per 10 minuti a causa dell'attacco DDoS, possiamo calcolare l'impatto finanziario come segue:

Impatto finanziario = Valore medio delle transazioni per minuto * Durata dell'inattività

= 1.500 €/min * 10 min

= 15.000 €

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.

conclusioni e soluzioni :

Per mitigare gli effetti di futuri attacchi DDoS, è possibile implementare azioni preventive come:

Utilizzo di servizi di mitigazione DDoS: Investire in servizi specializzati che possono rilevare e mitigare gli attacchi DDoS in tempo reale, proteggendo così l'applicazione web dalla congestione del traffico dannoso.

Distribuzione della rete: Utilizzare una rete distribuita di server e servizi per ridurre il rischio di un singolo punto di fallimento. Questo può includere l'utilizzo di Content Delivery Network (CDN) per distribuire il carico di lavoro e aumentare la resistenza agli attacchi.

Aggiornamenti di sicurezza: Mantenere costantemente aggiornati i software e i sistemi per correggere le vulnerabilità note e ridurre la superficie di attacco disponibile agli aggressori.

Monitoraggio attivo: Implementare sistemi di monitoraggio attivo per rilevare rapidamente gli attacchi DDoS in corso e rispondere prontamente con misure di mitigazione.

Pianificazione della capacità: Avere una pianificazione della capacità adeguata per gestire picchi di traffico inattesi, che potrebbe includere la disponibilità di risorse aggiuntive o l'espansione elastica dell'infrastruttura durante periodi di elevata attività.

Che cosa è un attacco di DDoS:

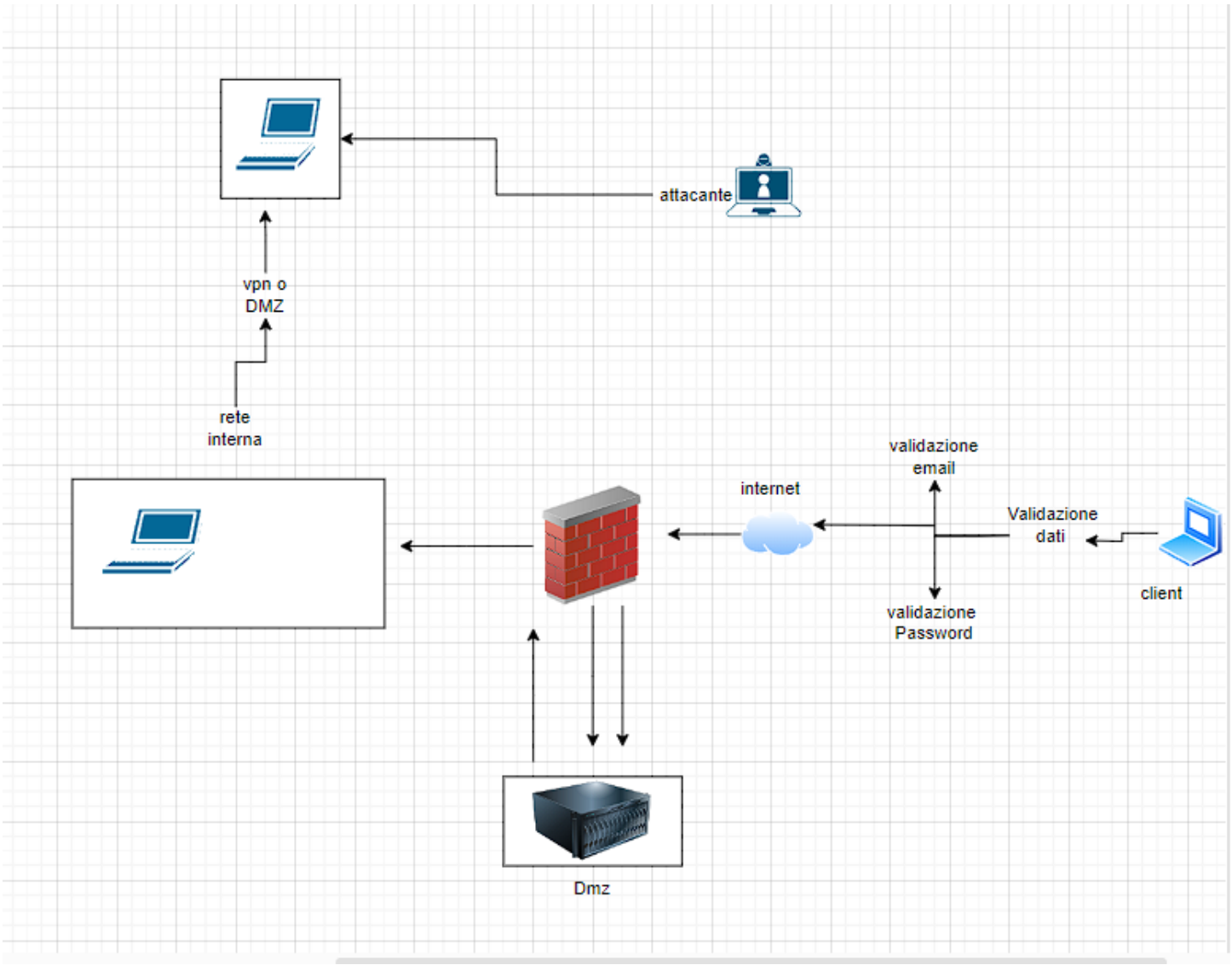
Un attacco DDoS è un tipo di attacco informatico in cui una vasta rete di dispositivi compromessi invia un'enorme quantità di traffico illegittimo a un server o un'applicazione web, sovraccaricandoli e rendendo il servizio o la risorsa online non disponibile agli utenti legittimi. L'obiettivo è negare l'accesso ai servizi online, causando interruzioni, perdite finanziarie e danni alla reputazione dell'azienda.

Gli attacchi DDoS possono avere gravi conseguenze, tra cui l'interruzione dei servizi online, la perdita di clienti, danni alla reputazione dell'azienda, perdite finanziarie e altro ancora. È importante implementare misure di protezione e mitigazione per difendersi dagli attacchi DDoS, come ad esempio l'utilizzo di servizi di mitigazione DDoS, la distribuzione della rete, e la pianificazione della capacità per gestire picchi di traffico inattesi.

3.Response

Poiché la priorità è prevenire la propagazione del malware sulla rete senza necessariamente rimuovere l'accesso dell'attaccante alla macchina infettata, è importante isolare l'applicazione Web infetta per impedire che il malware si diffonda ulteriormente. Una possibile soluzione potrebbe essere l'implementazione di una rete virtuale privata (VPN) o di una zona demilitarizzata (DMZ) per isolare l'applicazione infetta dal resto della rete. Questo consentirebbe all'attaccante di mantenere l'accesso alla macchina infetta mentre protegge il resto della rete dall'ulteriore diffusione del malware.

Ecco una possibile rappresentazione di questa soluzione:



Nella figura, la VPN o la DMZ isolano l'applicazione Web infetta, impedendo la propagazione del malware sulla rete interna protetta. Questa soluzione consente all'attaccante di mantenere l'accesso alla macchina infetta senza compromettere la sicurezza del resto della rete.

Che cosa è VPN e DMZ:

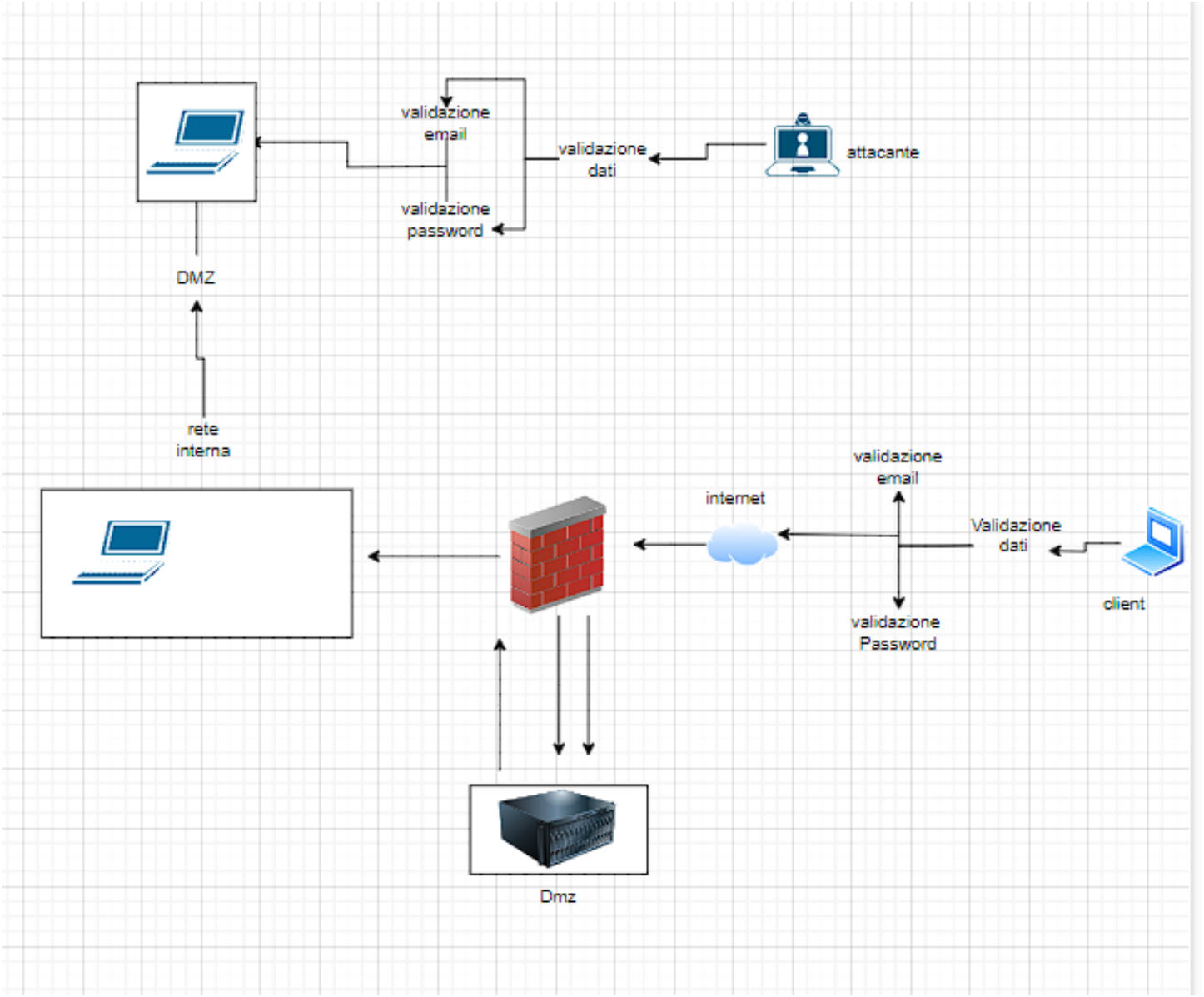
VPN (Virtual Private Network):

- Una VPN è una rete privata virtuale che permette di creare una connessione sicura e crittografata su una rete pubblica, come Internet.
- Essenzialmente, una VPN consente agli utenti di accedere in modo sicuro alla rete aziendale o a una rete privata da remoto, fornendo un tunnel crittografato attraverso cui passano i dati.
- Le VPN sono spesso utilizzate per garantire la privacy e la sicurezza durante la navigazione su Internet, per consentire l'accesso sicuro alle risorse aziendali da remoto e per creare connessioni sicure tra sedi geograficamente distanti.

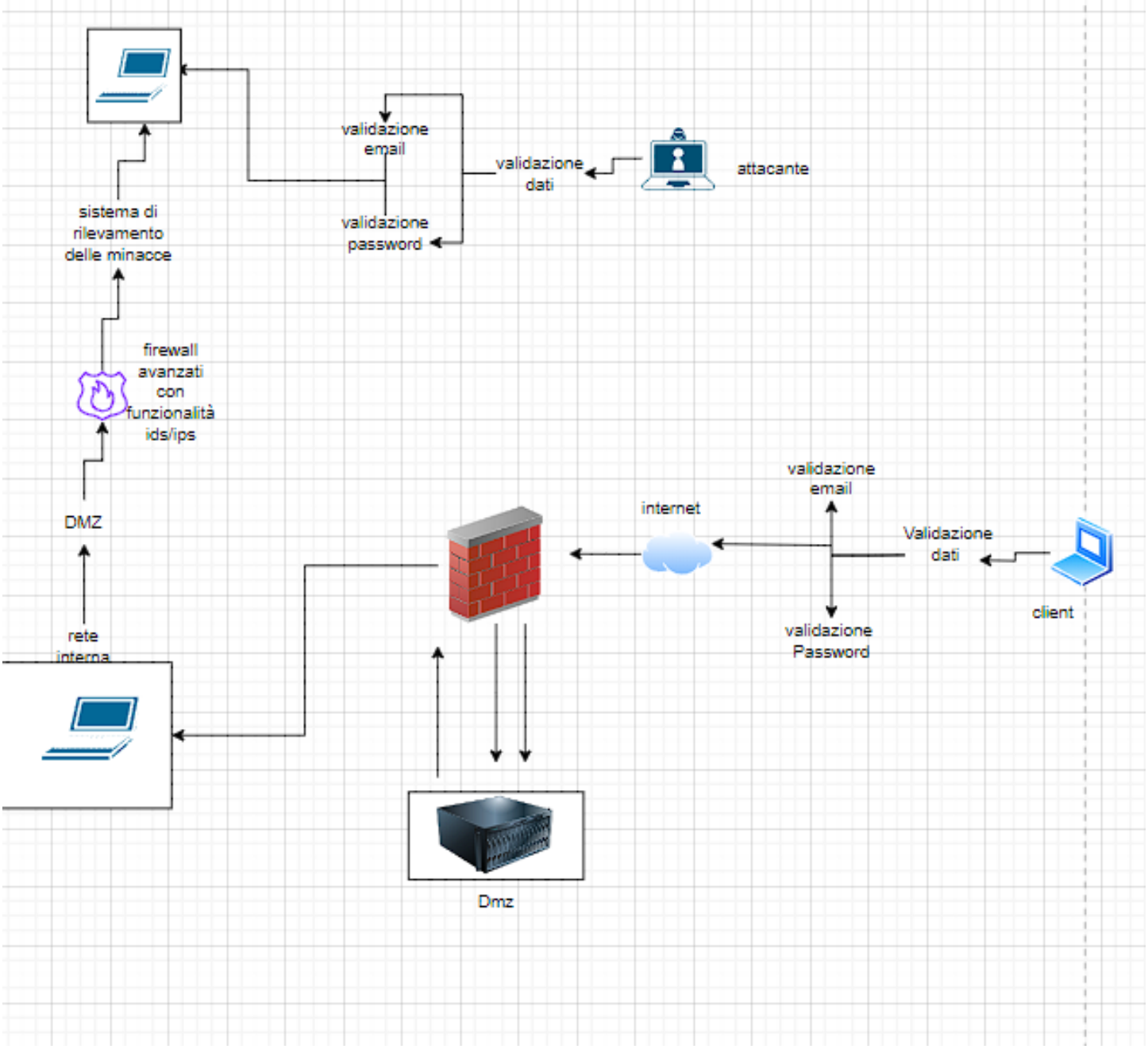
DMZ (Demilitarized Zone):

- Una DMZ è una porzione di rete localizzata tra la rete interna protetta di un'organizzazione e una rete esterna non fidata, come Internet.
- La DMZ è progettata per ospitare servizi pubblici o esposti, come server web, server di posta elettronica o server DNS. Questi servizi sono accessibili dall'esterno, ma isolati dalla rete interna per garantire una maggiore sicurezza.
- La DMZ viene spesso implementata con l'uso di firewall e regole di routing per controllare il traffico tra la rete interna, la DMZ e la rete esterna. Questo permette di proteggere la rete interna da potenziali minacce provenienti dall'esterno, mantenendo al contempo l'accessibilità ai servizi pubblici.

4.Soluzione completa



5-Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2 .



nel diagramma vediamo

- La VPN o la DMZ isolano l'applicazione Web infetta, impedendo la propagazione del malware sulla rete interna protetta.
- I firewall avanzati con funzionalità IDS/IPS monitorano e filtrano il traffico in ingresso e in uscita dall'applicazione infetta, identificando e bloccando attività sospette.

- I sistemi di rilevamento delle minacce (Threat Detection Systems) identificano comportamenti anomali o attività maliziose sulla rete, avvisando il personale della sicurezza per avviare azioni di mitigazione.