INDICE

PAG	TITOLO
1	traccia
2	creazione ambiente
2	azioni preventive
3	impatti sul business
5	response
6	conclusioni

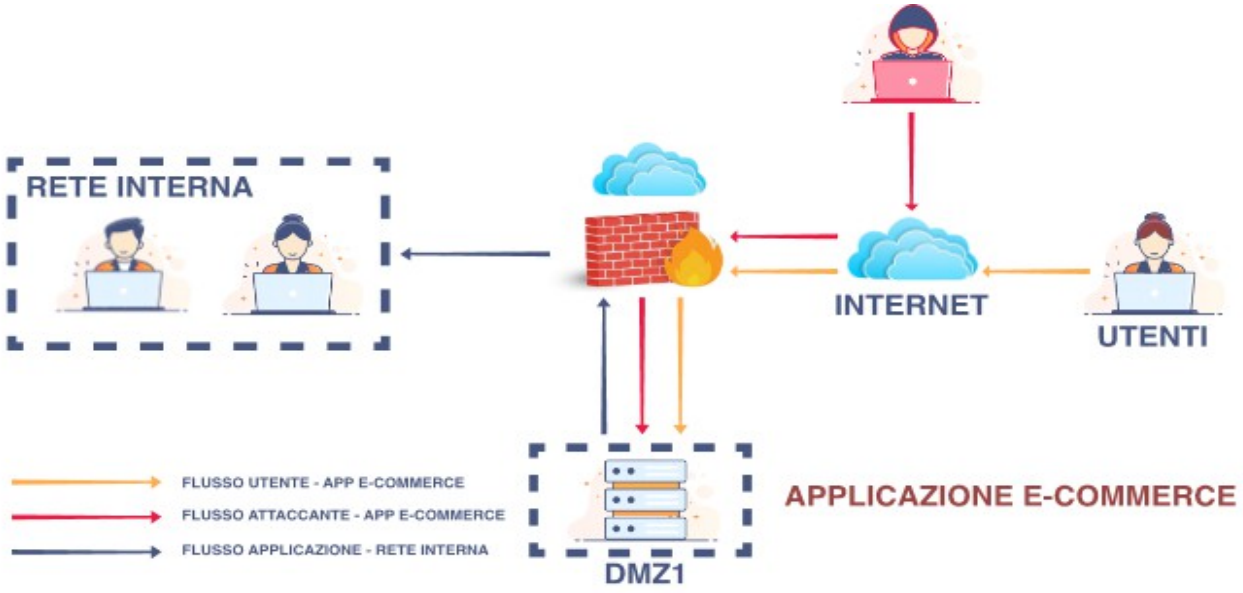
TRACCIA

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

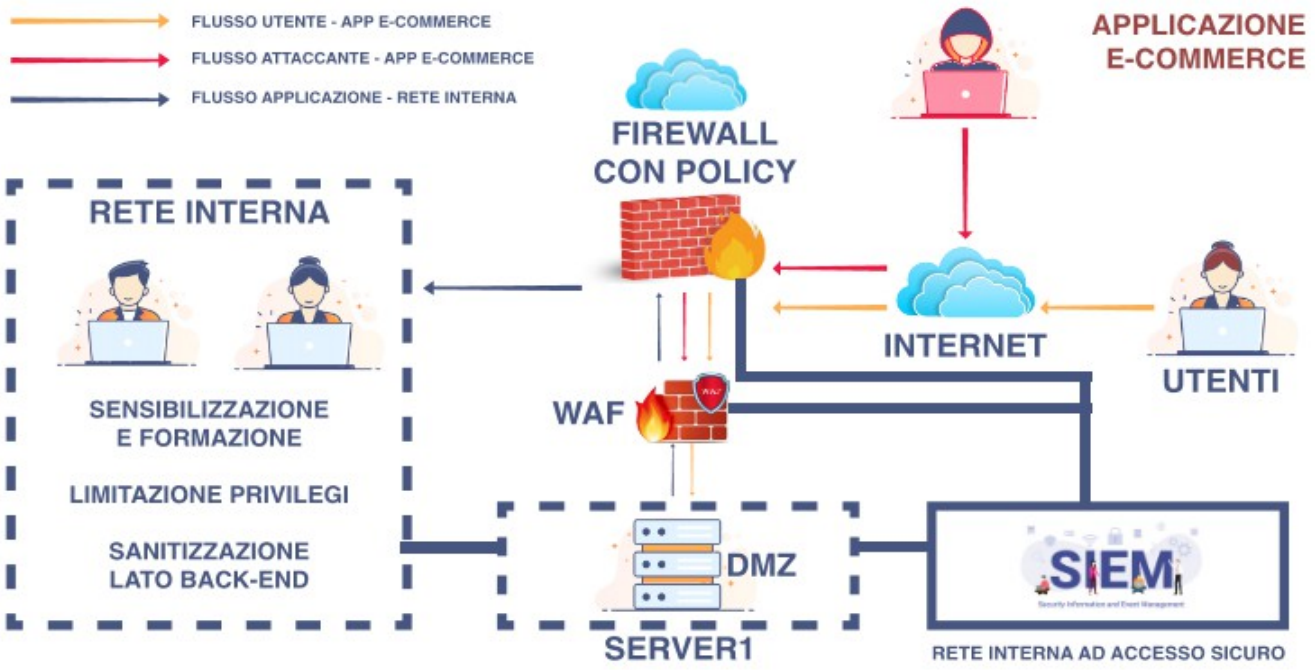
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE

Di seguito vengono riportate una serie di opzioni di azioni per prevenire attacchi XSS, SQLi ed in generale qualsiasi tipo di attacco alle Web App da parte di un utente malintenzionato, che possa essere sia all'interno che all'esterno dell'attività di e.commerce:

- **WEB APPLICATION FIREWALL (WAF)**: monitara il traffico e limita le richieste inviate alle applicazioni così da permettere l'accesso solamente agli utenti legittimi
- **VALIDAZIONE E SANITAZIONE DEGLI INPUT**: input validi sia sul lato client che sul lato server, accettando solo input che soddisfino determinati criteri. Rimozione o codificare caratteri speciali che possono essere utilizzati in attacchi sqli o xss.
- **HTTPS**: crittografere il traffico client-server. Protezione dati in transito.
- **AGGIORNAMENTI E PATCH**: aggiornamenti per prevenire attacchi con bug noti.
- **SENSIBILIZZAZIONE E FORMAZIONE**: formazione ocntinua degli sviluppatori e personale interno che hanno accesso ai vari end-point.
- **LIMITAZIONE DEI PRIVILEGI**: usare account con il minimo livello di privilegi necessario per svolgere il lavoro.
- **LOGGING E MONITORAGGIO**: utile mantenere loig dettagliati delle attività per una visione centralizzata della sicurezza, utilizzando sistemi SIEM, e monitorare le app ed i sistemi per individuare e reagire rapidamente a qualsiasi attività sospetta ed eventuali minacce o attacchi in corso.
- **VULNERABILITY ASSESSMENT**: fare continue campagne e periodici test dell'applicazione facendo dei Penetration Test per scoprire eventuali falle ed agire prima che possano venire sfruttate da malintenzionati.
- **DIFFERENTIAL BACKUP**: eseguire backup regolari dei dati e del codice dell'applicazione su sistemi di storage sicuri e testare regolarmente la procedura di ripristino.
  Soluzione meno dispendiosa a livello di tempoi in qunato permette di implementare solo dati che sono stati modificati dall'ultimo full backup che vengono copiati e salvati.
- **SISTEMI DI RILEVAMENTO E PREVENZIONE DELLE INTRUSIONI (IDS/ISP):** implementare IDS/IPS per rilevare comportamenti anomali o schemi di attacco e prendere azioni automaticamente per prevenire o mitigare gli attacchi



IMPATTI SUL BUSINESS

Si esamina la situazione in cui la Web App viene contrassegnata come bersaglio di un attacco DDoS, ovvero un Distributed Denial of Service, una tipologia di attacco coordinato dove molteplici macchine inviano contemporaneamente grandi quantità di pacchetti allo stesso indirizzo IP, generando una enorme quantità di traffico con l'obiettivo di intasare la rete ed impedire il corretto funzionamento del servizio.

Si richiede di calcolare l'impatto sul business considerando che in media ogni minuto gli utenti spendono 1500 € sulla piattaforma di e-commerce.

Nel nostro caso l'attacco è riuscito ad impedire il corretto funzionamento per 10 minuti.
Sappiamo anche che gli utenti spendono in media 1500 € al minuto.

1500 x 10=15000 €

Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica: Accettazione del rischio o riduzione.

Non abbiamo informazioni precise riguardo:

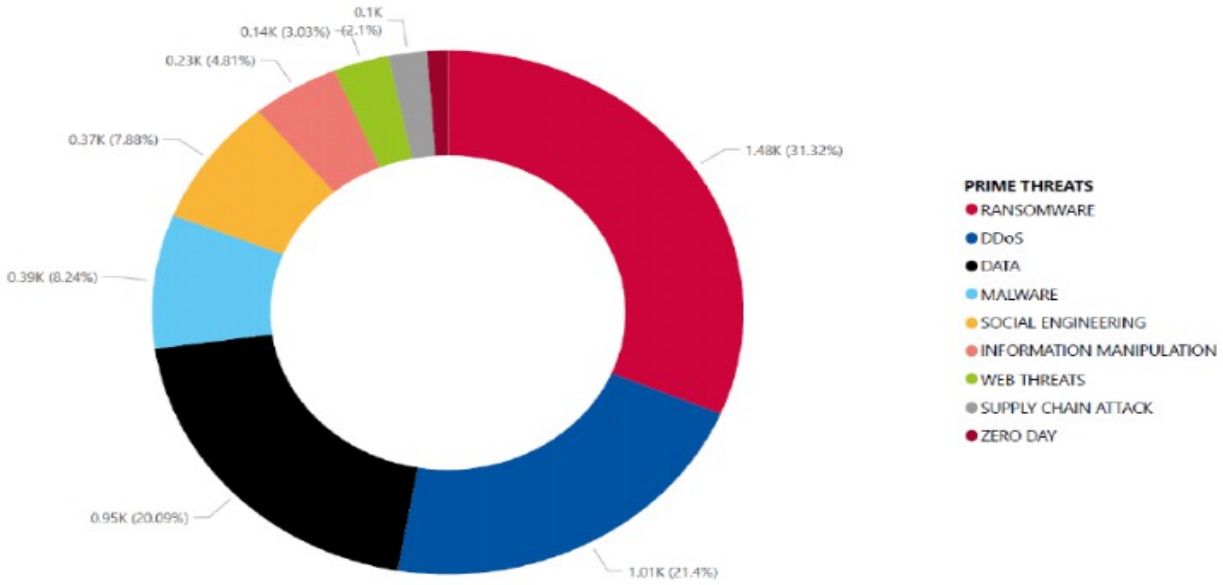
- il settore dell'attivitò
- la categoria merceologica
- collocazione nel commercio
- situazione geopolitica

Si considera perciò la perdita di 15000 € in dieci minuti → attività media entità con un budget non elevatissimo da investire in security operations e BCP.

Un'accettazione del rischio potrebbe non essere una buona opzione trattandosi di hosting che deve rendere disponibile il proprio servizio alla clientela e rispettare la triade CIA.

Quanto riportato nel 2023 dai report di ENISA, l'attacco Ddos è secondo in frequenza solo ai ransomware.

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)



Gli attacchi Ddos sono diventati più complessi, spostandosi verso reti mobili e dispositivi internet of the Things (IoT).
Dal report Imperva Global Ddos Threat Landscape del 2023 riporta un incremento dell'82% dewgli attacchi Ddos a livello applicazione nel 2022 rispetto al 2021, con attacchi al settore dei servizi finanziari cresciuti del 121% anno su anno.
In Italia un terzo sono di tipo Ddos: aumento collegato all'attivismo e alla guerra informatica, che mirano ad interropmere le operazioni di un'entità per attirare l'ìattenzione mediatica su cause politiche o sociali.

Bisogna perciò implementare le difese per ridurre il rischio, anche a costo di andare oltre la cifra dei 15000 € persi in dieci minuti.

SOLUZIONI PROPOSTE:

- **cambiare DNS**: distribuzione del carico di traffico tra più server (Load Balancing) incrementando la resilienza dell'architettura contro gli attacchi.
  L'uso di servizi di DNS secondario (o di Failover) garantisce che il dominio rimanga online anche se il provider primario subisce una interruzione.
- **Strumenti di monitoraggio del traffico in tempo reale**: rilevano e prevengono picchi di traffico anomali, così da reagire prontamente prima di arrivare a danni maggiori
- **introdurre un servizio Cloudflare**: mitiga gli attacchi Ddos per i siti web Htto/Https, inclusa gratuitamente in tutti i piani di servizio delle applicazioni weeb di Cloudflare.
  Particolarità di mitigare gli attacchi in una manciata di secondi dando così possibilità di risposta rapida ad un eventuale attacco.
- **Logging e monitoraggio**: visione centralizzata della sicurezza con sistemi SIEM
- **inserimento di piattafomre di Threat Intelligence**

Effettuare una valutazione dei danni che riguardano l'attività e accordi commerciali con altri aziende.

Le contromisure sono utili a limitare i rischi e a non permettere ad eventuali minacce esterne/interne di tenere giù i sistemi a lungo:

- minimizzare temmpistiche di ripristino
- mantenere integrità del database e dati sensibili

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.

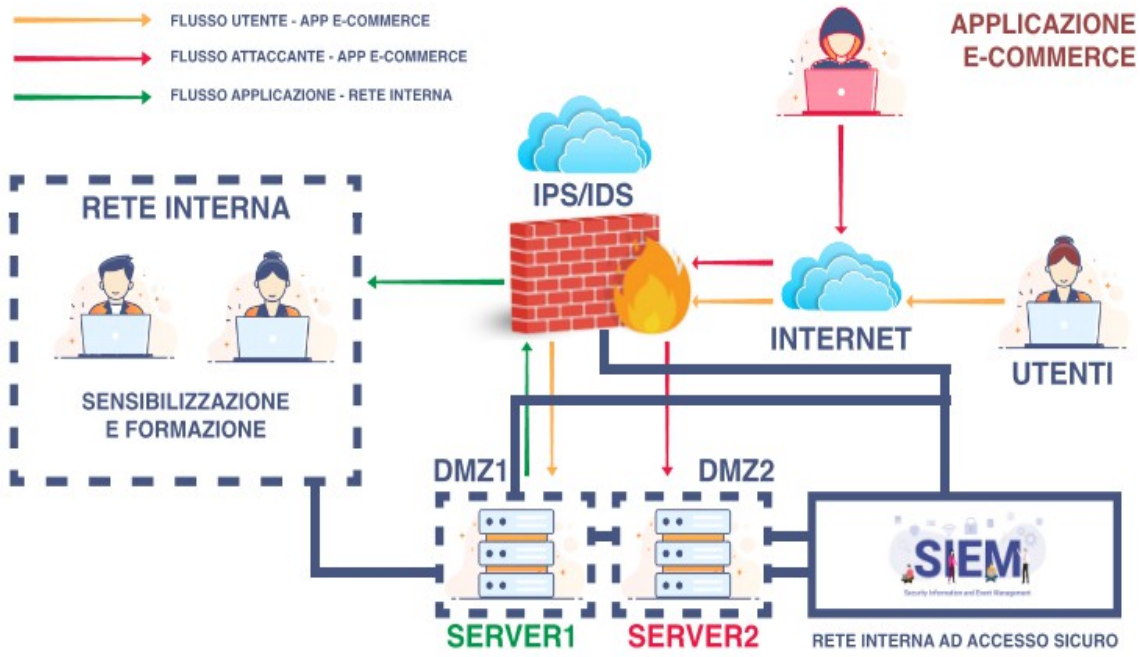
- Provvedere a **segmentare** la rete seguendo i principi dell'isolamento e della rimozione del servizio infetto per fare in modo che i danni siano contenuti.
- Procedere a separare la rete interna dal resto dello schema di rete, assicurando che la rete diventi un ambiente isolato e non raggiungibile da internet né dalla Web App infetta → Rete in Quarantena.

Si crea così una RETE AD HOC: con le dovute configurazione a livello network si crea un sistema di contenimento, il malware risulta separato dal resto della rete ed incapace di riproduris e diffondersi.
Questo ambiente ci permette di studiare ed analizzare il comportamento in un secondo momento senza che si propaghi sulla rete interna.

- Switch sul server2 con i suoi backup e garantisce l'erogare del servizio mantenendone la continuità operativa dell'hosting.

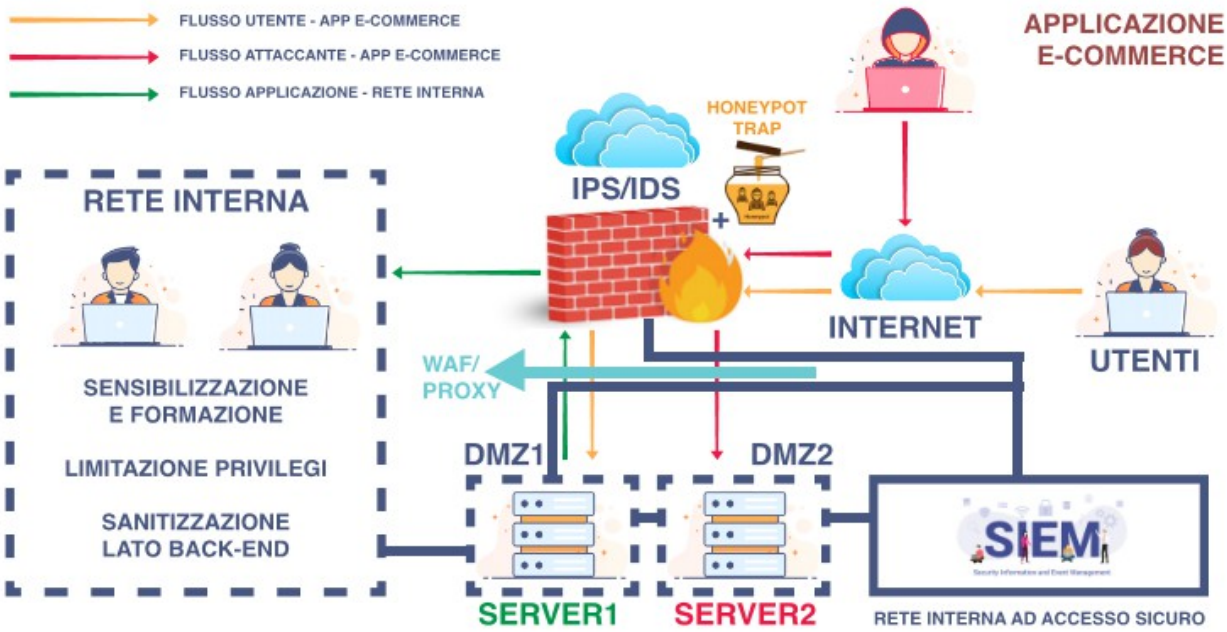
Si potrebbe implementare

- con un **IPS/IDS** verificando se il dispositivo che fa da firewall ne supporta l'implementazione.
- con sistema **SIEM**, con sonde sia sui server che a livello di rete ed anche a livello di end-point per rilevare comportamenti anomali e prendere azioni automatiche per prevenire o mitigare gli attacchi.
- Agire sulla **ridondanza dei server e dei network** per ottenere una maggiore resilienza e tolelranza agli errori, assicurarsi che ci sia più di un server ad ospitarla. Cosi nel caso di un fallimento di uno dei server, si puà sempre continuare ad erogare il servizio con gli altri presenti (Failover Cluster).
- **Bilanciare il carico** per evitare single point of failure che renderebbero l'applicazione inaccessibile.
  Implemtanre quidni con un Raid. Raid-1 → Raid-5
- **Differential Backup** che implementa solo dati che sono stati modificati dall'ultimo full backup
  Il componente su cui si esegue il backup deve essere staccata dal sistema a ifne backup e non far parte di alcuna rete.
- Servirsi di un **Honeypot** che è un sistema che sembra far parte della rete ma è in realtà isolata e monitorata.
  Funzione di attirare gli attaccanti che pensando di accedere a parti sensibili della rete, si riveleranno e verranno intrappolati. Ciò permette di distogliere l'attenzione degli attaccanti dalle risorse reali ed agire.
  Un buon posizionamento può essere nella DMZ o in una subnet.
  Diversi tipi di Honeypot:
  bassa interazione, simulano servizi o applicazioni → alta interazione, sistemi complessi e interagiscono con l'attaccante
- configurare un **Proxy** per filtrare contenuti, nasconde l'indirizzo IP effewttivo di un utente e proteggere la rete interna da accessi diretti.
  Configurandolo come un gateway, tutti i dati lo attraverseranno permettondi di essere analizzati e filtrare il traffico sospetto.
- Soluzione costosa è creare un **Data Center** geograficamente distribuiti, distribuento l'infrastruttura su più data center in diverse aree geografiche per proteggerla da disastri naturali o guasti di rete localizzati.
- Integrare software che utilizzano l'**intelligenza artificiale** e il **machine learning** per rilevare e risposndeere a minacce in tempo reale nella rete.
  Questo è permesso attraverso una analisi comportamentale dove possono identificare attività sospette o anomale che potrebbe indicare la presenza di malware o altri tipi di attacchi.



CONCLUSIONI

Unire la soluzione preventiva e la response.



Nel caso l'isolamento non basti, si dovrà procedere con la **RIMOZIONE DEL SISTEMA INFETTO**.
Bisogna smaltire o recuperare i dischi di storage su cui si trova il sistema attaccato.
I metodi:

- Purge: rimozione dei dati con metodi fisici → magneti
- Destroy: distruzione totale del disco → alte temperature, disintegrazione, ..
- Clear: rimozione dei dati → factory reset o sovvrascrizione

Si può ricorrere al DRAAS (Disaster Recovery As a Service).
I cloud provider mettono a disposizione una infrastruttura in cloud che viene immediatamente attivata in caso di disastro sul sito primario.
Svantaggi sono i tempi di latenza del cambio da sito primario al secondario-
Vantaggio è che è un servizio che si paga sono in caso di necessità.