

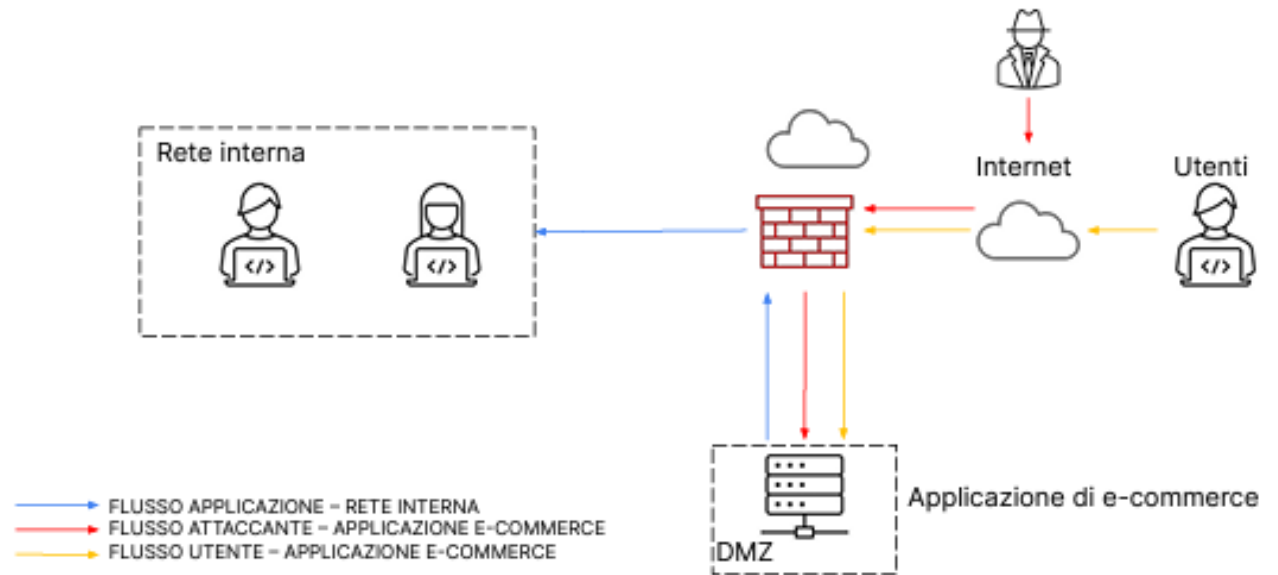
# W20D4 Esercizio modulo5

IMPLEMENTAZIONE DI MISURE DI SICUREZZA PER PROTEZIONE DI  
UN'APPLICAZIONE E-COMMERCE: PREVENZIONE, MITIGAZIONE E RISPOSTA  
AGLI ATTACCHI INFORMATICI

Garzoni Michele

# Architettura di rete

L'applicazione di e-commerce deve essere accessibile agli utenti tramite Internet per consentire loro di effettuare acquisti sulla piattaforma. La rete interna può essere raggiunta dalla DMZ a causa delle regole impostate sul firewall. Pertanto, se il server nella DMZ viene compromesso, un attaccante potrebbe potenzialmente accedere alla rete interna.



# Azioni Preventive contro Attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS)

PROPOSTE DI IMPLEMENTAZIONE

# 1. Web Application Firewall (WAF)

- I Web Application Firewall (WAF) consentono di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione. Il WAF consentirà di definire e gestire le regole per evitare minacce a Internet, tra cui indirizzi IP, intestazioni HTTP, corpo HTTP, stringhe URI, scripting tra siti (XSS), inserimento SQL e altre vulnerabilità definite da OWASP. Il firewall dell'applicazione Web viene distribuito per proteggere le applicazioni Web e raccogliere i log di accesso per la conformità e l'analisi.

# Perché la sicurezza WAF è importante?

- I firewall delle applicazioni Web aiutano a proteggere le applicazioni distribuite nel cloud pubblico, on premise e in ambienti multcloud con controlli dell'accesso basati sui dati di geolocalizzazione, sulla lista di inclusione e sugli indirizzi IP in backlist, sull'URL HTTP (Hypertext Transfer Protocol Uniform Resource Locator) e sull'intestazione HTTP. Le WAF possono identificare e bloccare il traffico bot dannoso con un set avanzato di metodi di verifica, inducendo JavaScript, Completely Automated Public Turing Test to tell Computers and Humans Apart (CAPTCHA), interpretazione dei dispositivi e algoritmi di interazione umana. I WAF proteggono le applicazioni che si interfacciano con Internet dagli attacchi a seguito dell'intelligence sulle minacce integrate che aggrega più origini e regole di rilevamento Open Web Application Security Project (OWASP).

## 2. Validazione e Sanitizzazione degli Input

- ▶ Assicurarsi che tutti gli input forniti dagli utenti siano validati sia sul lato client che sul lato server, accettando solo input che soddisfano determinati criteri.
- ▶ Rimuovere o codificare caratteri speciali che possono essere utilizzati in attacchi SQLi o XSS.

# Perchè validare l'input utente è importante?

- ▶ La convalida dell'input utente è importante per la sicurezza. Quando si limitano i valori che gli utenti possono immettere nei moduli, è possibile ridurre la possibilità che un utente possa immettere un valore che possa compromettere la sicurezza del sito.

### 3. Utilizzo di protocolli criptati (HTTPS)

- ▶ Utilizzare HTTPS per crittografare il traffico tra il client e il server, proteggendo i dati in transito.



# Perchè è importante usare HTTPS?

- ▶ **Sicurezza dei Dati:** HTTPS crittografa i dati trasmessi tra il client (utente) e il server, proteggendo le informazioni sensibili come password, dati personali e numeri di carte di credito da intercettazioni e attacchi man-in-the-middle.
- ▶ **Autenticità e Integrità:** HTTPS garantisce che i dati non siano stati alterati durante il trasferimento e conferma l'identità del sito web tramite certificati SSL/TLS. Questo impedisce attacchi di phishing e assicura agli utenti di interagire con il sito legittimo.
- ▶ **SEO e Ranking:** I motori di ricerca come Google preferiscono i siti HTTPS rispetto agli HTTP, migliorando il posizionamento nei risultati di ricerca. Utilizzare HTTPS può quindi aumentare la visibilità e il traffico del sito.
- ▶ **Affidabilità e Fiducia degli Utenti:** Gli utenti si sentono più sicuri e fiduciosi nel navigare e interagire con siti che utilizzano HTTPS. I browser moderni avvertono gli utenti quando visitano un sito non sicuro (HTTP), il che può dissuaderli dal proseguire la navigazione.
- ▶ **Conformità Normativa:** Molte normative sulla protezione dei dati, come il GDPR in Europa, richiedono l'uso di connessioni sicure per proteggere i dati personali. Utilizzare HTTPS aiuta a rispettare queste leggi e a evitare sanzioni.

# Aggiornamenti e Patch

- ▶ Necessità di mantenere i sistemi e servizi aggiornati.
- ▶ Discussione delle strategie di aggiornamento.

# Perchè è importante controllare gli aggiornamenti?

- ▶ **Sicurezza:** Gli aggiornamenti e le patch correggono vulnerabilità che potrebbero essere sfruttate per attacchi informatici. Mantenere il sistema aggiornato protegge contro exploit, malware e accessi non autorizzati.
- ▶ **Compatibilità:** Aggiornare garantisce che il sistema rimanga compatibile con altre tecnologie e software, riducendo problemi di integrazione e funzionalità.
- ▶ **Supporto:** I fornitori di software offrono supporto per le versioni aggiornate. Utilizzare versioni obsolete può significare perdere l'accesso a risorse critiche e assistenza tecnica.
- ▶ **Prestazioni:** Le nuove versioni del software spesso includono miglioramenti delle prestazioni e dell'efficienza, rendendo il webserver più veloce e affidabile.

# Strategie di aggiornamento

- ▶ **Pianificazione regolare:** Stabilire un calendario per aggiornamenti e patch, ad esempio settimanalmente o mensilmente, per garantire che il sistema sia sempre protetto e aggiornato.
- ▶ **Test preliminari:** Prima di applicare aggiornamenti su un sistema di produzione, testarli in un ambiente di staging per identificare potenziali problemi senza impattare i servizi in produzione.
- ▶ **Backup:** Effettuare backup completi del sistema prima di applicare qualsiasi aggiornamento, per assicurarsi di poter ripristinare la versione precedente in caso di problemi.
- ▶ **Automazione:** Utilizzare strumenti di gestione delle patch e degli aggiornamenti automatici per ridurre il rischio di errori umani e garantire che nessun aggiornamento critico venga dimenticato.
- ▶ **Monitoraggio continuo:** Implementare sistemi di monitoraggio per rilevare e notificare automaticamente la disponibilità di nuove patch e aggiornamenti, garantendo una risposta rapida a nuove vulnerabilità.

## 6. Limitazione dei Privilegi

- ▶ Le connessioni al database dovrebbero usare account con il minimo livello di privilegi necessario per svolgere il lavoro.

# Perchè è importante limitare i privilegi?

- ▶ Utilizzare account con privilegi minimi significa che, anche se un malintenzionato dovesse riuscire a ottenere l'accesso all'account, le azioni che può compiere sarebbero limitate. Ad esempio, un account con privilegi di sola lettura non può modificare o cancellare dati.
- ▶ Se un account con privilegi elevati viene compromesso, un attaccante potrebbe eseguire operazioni dannose come l'eliminazione di tabelle, la modifica di dati critici o la creazione di account aggiuntivi. Limitando i privilegi, si riduce il potenziale danno che un attacco potrebbe causare.
- ▶ Gli errori umani sono una delle principali cause di incidenti di sicurezza. Limitare i privilegi degli account riduce il rischio che un utente legittimo commetta un errore che possa avere gravi conseguenze, come la cancellazione accidentale di dati.
- ▶ Il Principio del Minimo Privilegio suggerisce che ogni componente di un sistema dovrebbe avere solo i privilegi strettamente necessari per eseguire le proprie funzioni. Questo approccio riduce le opportunità di abuso e limita gli impatti di eventuali violazioni.

# Logging e Monitoraggio

- Mantenere log dettagliati delle attività per una visione centralizzata della sicurezza e monitorare le app e i sistemi per individuare e reagire rapidamente a qualsiasi attività sospetta ed eventuali minacce o attacchi in corso.

# Perchè è importante il logging?

- ▶ I log permettono di monitorare tutte le attività svolte sul server, compresi accessi, modifiche ai file, tentativi di connessione, e altro. Questo aiuta a individuare rapidamente attività anomale o non autorizzate che potrebbero indicare un attacco in corso.
- ▶ Grazie ai log, è possibile identificare tentativi di attacco, come attacchi brute force, SQL Injections, o altri tipi di attacchi. I log forniscono tracce delle azioni sospette che possono essere analizzate per capire la natura dell'attacco e per prendere misure adeguate.
- ▶ In caso di violazioni della sicurezza, i log forniscono una cronologia dettagliata delle attività, permettendo agli amministratori di ricostruire l'accaduto, capire come l'attacco è avvenuto, e individuare i punti deboli del sistema.
- ▶ I log documentano chi ha fatto cosa e quando, fornendo una traccia di audit che è cruciale per gestire le modifiche nel sistema, rilevare errori umani e assicurarsi che le policy aziendali vengano rispettate.
- ▶ Molte normative e standard di settore (come GDPR, HIPAA, PCI-DSS) richiedono il mantenimento di log dettagliati per garantire la protezione dei dati e la trasparenza delle operazioni. I log aiutano a dimostrare la conformità durante gli audit.



# Vulnerability Assessment

- ▶ Condurre campagne continue e test periodici sull'applicazione facendo dei penetration test per scoprire eventuali falle e porvi rimedio prima che possano essere sfruttate da malintenzionati.

# Perchè è importante un VA Periodico?

- ▶ Questi test permettono di individuare le potenziali vulnerabilità nel sistema e nelle applicazioni. Le vulnerabilità possono essere causate da errori di programmazione, configurazioni non sicure o altre debolezze che potrebbero essere sfruttate da attaccanti.
- ▶ Scoprire le vulnerabilità prima che vengano scoperte dagli attaccanti permette di prendere misure preventive. Questo riduce significativamente il rischio che i criminali informatici possano sfruttare queste falle per accedere non autorizzatamente al sistema.
- ▶ Molte normative e standard di sicurezza, come ad esempio il GDPR in Europa o il PCI DSS per le transazioni con carta di credito, richiedono la conduzione di test periodici di sicurezza. Adempiere a queste normative non solo protegge i dati degli utenti, ma evita anche sanzioni legali.

# Backup periodici

- ▶ Eseguire backup regolari dei dati e del codice dell'applicazione su sistemi di storage sicuri e testare regolarmente la procedura di ripristino.

# Perchè i backup sono importanti?

- ▶ I dati sono preziosi in un web commerce, inclusi ordini dei clienti, informazioni di pagamento e dati sensibili. I backup permettono di ripristinare i dati in caso di perdita per qualsiasi motivo (errori umani, problemi tecnici, attacchi informatici, etc.).
- ▶ Se il sito web dovesse andare offline a causa di un guasto hardware, di un attacco informatico o di un errore di configurazione, i backup consentono di ripristinare rapidamente il sito e ridurre al minimo il downtime, mantenendo così la continuità operativa.
- ▶ Molte normative (come il GDPR in Europa) richiedono che i dati personali siano adeguatamente protetti e mantenuti sicuri. Avere backup regolari è una misura importante per garantire la sicurezza dei dati e rimanere conformi alle normative vigenti.
- ▶ Gli errori umani possono accadere, come l'eliminazione accidentale di dati importanti. Avere backup regolari permette di recuperare rapidamente i dati persi e limitare il danno.

## Sistemi di Rilevamento e Prevenzione delle Intrusioni (IDS/IPS)

- Implementare soluzioni IDS/IPS per rilevare comportamenti anomali o schemi di attacco e prendere azioni automatiche per prevenire o mitigare gli attacchi.

# Perchè soluzioni IDS/IPS sono importanti?

- ▶ Un web commerce gestisce informazioni sensibili dei clienti, come dati di pagamento, informazioni personali e storico degli acquisti. Gli IDS/IPS aiutano a proteggere queste informazioni da accessi non autorizzati o tentativi di furto di dati.
- ▶ I commerce online sono spesso bersagliati da frodi, come tentativi di accesso fraudolento agli account dei clienti, tentativi di utilizzo di carte di credito rubate o altre attività fraudolente. Gli IDS/IPS possono rilevare modelli anomali di accesso e comportamento che potrebbero indicare una possibile frode in corso.
- ▶ È essenziale mantenere il web commerce operativo e accessibile in modo continuo. Gli attacchi di tipo DoS (Denial of Service) possono bloccare o rallentare il servizio per gli utenti legittimi. Gli IDS/IPS possono rilevare e mitigare questi attacchi, aiutando a mantenere la disponibilità dei servizi.
- ▶ Molte normative e standard di sicurezza, come il GDPR in Europa o il PCI-DSS per la gestione delle informazioni di pagamento, richiedono misure di sicurezza robuste, tra cui la protezione con IDS/IPS, per garantire la conformità legale e ridurre il rischio di sanzioni.
- ▶ Gli IDS/IPS monitorano costantemente il traffico di rete e possono individuare in modo precoce segnali di attività sospette o di possibili attacchi informatici. Questo permette agli amministratori di rete di reagire rapidamente per mitigare il danno potenziale.
- ▶ I commerce online devono essere costantemente aggiornati e protetti contro nuove vulnerabilità e minacce emergenti. Gli IDS/IPS giocano un ruolo cruciale nel rilevare e gestire queste vulnerabilità prima che possano essere sfruttate da malintenzionati.

# Impatti sul business

CALCOLO DELL'IMPATTO SUL BUSINESS DI UN ATTACCO DDOS

# Impatto sul Business di un Attacco DDoS

## Descrizione dello scenario

- ▶ L'applicazione web subisce un attacco DDoS esterno, rendendo il servizio non raggiungibile per 10 minuti.
- ▶ Gli utenti spendono in media 1.500 € al minuto sulla piattaforma di e-commerce.
- ▶ in totale, gli utenti avrebbero speso 15.000 € in 10 minuti.

## Impatto economico

- ▶ Durata dell'attacco: 10 minuti
- ▶ Perdita finanziaria: **15.000 €**



# Valutazione delle Azioni Preventive

## Accettazione del Rischio:

Consiste nel non implementare misure preventive specifiche contro attacchi DDoS.

- ▶ **Vantaggi:** Costi minimi immediati.
- ▶ **Svantaggi:** Potenziali perdite finanziarie e danni all'immagine.

## Riduzione del Rischio:

Consiste nell'implementazione di soluzioni e misure preventive contro attacchi DDoS.

- ▶ **Utilizzo di servizi anti-DDoS:** Contratti con provider che offrono protezione DDoS
- ▶ **Configurazioni di firewall avanzate:** Filtraggio del traffico per bloccare attacchi.
- ▶ **Monitoraggio e risposta:** Implementazione di sistemi per rilevare e mitigare attacchi in tempo reale.

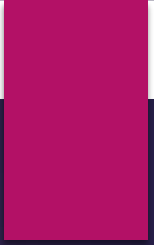
# Conclusioni

La protezione contro attacchi DDoS è cruciale per mantenere la continuità operativa e la fiducia degli utenti nella piattaforma di e-commerce. L'implementazione di misure contro gli attacchi Ddos porterebbero a seguenti pro e contro:

I benefici sono la riduzione della probabilità e dell'impatto degli attacchi DDoS.

Gli svantaggi sono il necessario investimento in tecnologie e servizi di sicurezza aggiuntivi.

L'azione consigliata è di **considerare la riduzione del rischio implementando misure preventive.**



# Response ad un infezione malware sulla web app

DESCRIZIONE DELL'INCIDENT RESPONSE ALL'INFEZIONE

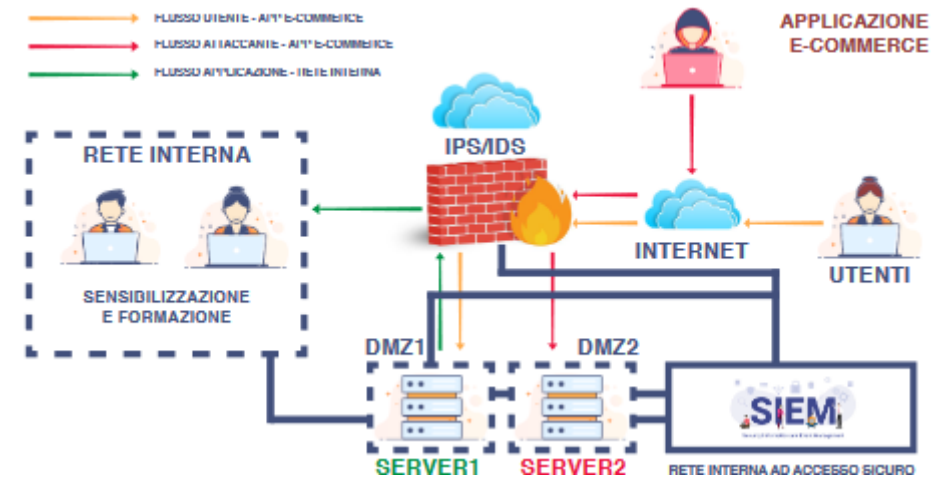
# Gestione di un Caso di Malware e Strategie di Sicurezza

## Introduzione:

In questo caso, dato che l'applicazione è stata già infettata dal malware, è stata previamente implementata una segmentazione di rete. Questo include l'assegnazione di diversi livelli di sicurezza alle varie aree della rete, come la DMZ (Demilitarized Zone), che espone i servizi accessibili da Internet.

La strategia più efficace è isolare il server1 infetto dalla rete principale e posizionarlo in una "rete di quarantena". Questa segmentazione permette di separare il sistema infetto dagli altri computer sulla rete, prevenendo la propagazione del malware e consentendo un'analisi del comportamento del malware in un momento successivo.

## Figura dell'architettura di rete



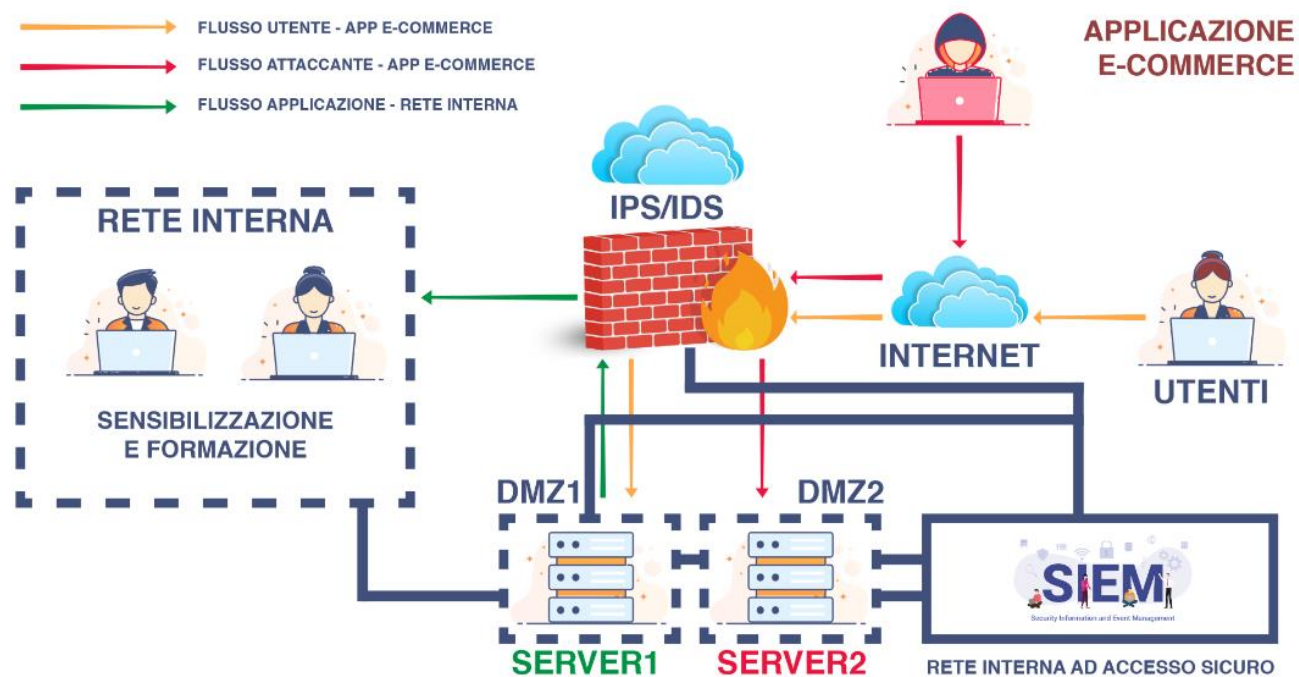
# Gestione di un Caso di Malware e Strategie di Sicurezza

- ▶ Nel frattempo, si passa al server2, il quale dispone di backup completi e può continuare a erogare il servizio per garantire la continuità operativa dell'hosting.
- ▶ Per migliorare ulteriormente la sicurezza, sarebbe consigliabile verificare se il dispositivo firewall supporta l'implementazione di un IPS/IDS (Intrusion Prevention System/Intrusion Detection System).
- ▶ Inoltre, un SIEM (Security Information and Event Management) sarebbe altamente consigliabile. Questo sistema potrebbe integrare un'intelligenza minaccia che monitora sia i server che la rete, oltre agli endpoint, per rilevare comportamenti anomali o schemi di attacco e prendere azioni preventive automatiche.

# Altre azioni preventive utili includono

- ▶ Implementare ridondanza dei server e dei network per aumentare la resilienza e la tolleranza agli errori dell'applicazione web, ad esempio attraverso failover cluster e bilanciamento del carico.
- ▶ Eseguire backup differenziali regolari dei dati e del codice dell'applicazione su sistemi di storage sicuri, con test regolari della procedura di ripristino.
- ▶ Configurare un proxy per filtrare il traffico internet e proteggere la rete interna da accessi diretti.
- ▶ Valutare l'implementazione di data center geograficamente distribuiti per proteggere l'infrastruttura da disastri naturali o guasti di rete locali.
- ▶ Esplorare soluzioni di sicurezza avanzata basate su AI e machine learning

# Esempio di architettura di rete



# Introduzione

Nel caso si volesse procedere con una modifica più aggressiva si possono considerare le seguenti soluzioni



# Ridondanza dei Server e dei Network

- ▶ Implementare failover cluster per garantire che il servizio possa continuare anche in caso di guasto di uno dei server.
- ▶ Progettare la rete con percorsi ridondanti per evitare i single point of failure che potrebbero rendere l'applicazione inaccessibile.
- ▶ Utilizzare RAID (ad es. RAID-1 o RAID-5) per garantire la continuità del servizio hosting e migliorare le prestazioni di lettura.

# Differential Backup

- ▶ Eseguire backup regolari dei dati e del codice dell'applicazione su sistemi di storage sicuri.
- ▶ Testare regolarmente la procedura di ripristino.
- ▶ Il differential backup copia solo i dati modificati dall'ultimo full backup, riducendo il tempo e la quantità di dati copiati.
- ▶ Staccare ogni componente di backup dalla rete a fine procedura.

# Honeypot

- ▶ Implementare un honeypot come parte della strategia di sicurezza.
- ▶ Il honeypot è una risorsa di sistema isolata e monitorata che simula parti sensibili della rete per attirare e intrappolare gli attaccanti.
- ▶ Posizionarlo in una zona ben monitorata ma apparentemente attraente per gli attaccanti, come la DMZ o una subnet isolata.

# Configurazione di un Proxy

- ▶ Utilizzare un proxy come intermediario per le richieste di client verso altri server.
- ▶ Filtrare contenuti, nascondere l'indirizzo IP degli utenti e proteggere la rete interna da accessi diretti.
- ▶ Configurare il proxy come gateway obbligato per analizzare e filtrare il traffico sospetto.

# Data Center Geograficamente Distribuiti

- ▶ Distribuire l'infrastruttura su più data center in diverse aree geografiche per ridurre il rischio di interruzioni causate da disastri naturali o guasti di rete locali. Questa soluzione è più costosa ma può essere cruciale per attività con elevate esigenze di continuità operativa.

# Darktrace

- ▶ Utilizzare soluzioni basate su intelligenza artificiale e machine learning come Darktrace per rilevare e rispondere in tempo reale a minacce nella rete.
- ▶ Questi sistemi analizzano il traffico alla ricerca di comportamenti anomali e collaborano spesso con dispositivi di sicurezza come i firewall.

# Response ad un infezione malware sulla web app

MODIFICA PIÙ AGGRESSIVA DELL'INFRASTRUTTURA DI RETE

# Rimozione del Sistema Infetto e Gestione degli Incidenti

Nel caso in cui l'isolamento e le altre misure indicate nel punto precedente non siano sufficienti, una delle modifiche più aggressive potrebbe essere la rimozione del sistema infetto. Quando diventa necessario eliminare ogni traccia dell'incidente, è cruciale gestire adeguatamente i dischi di storage contenenti il sistema attaccato.

Esistono diversi metodi per la rimozione sicura dei dati:

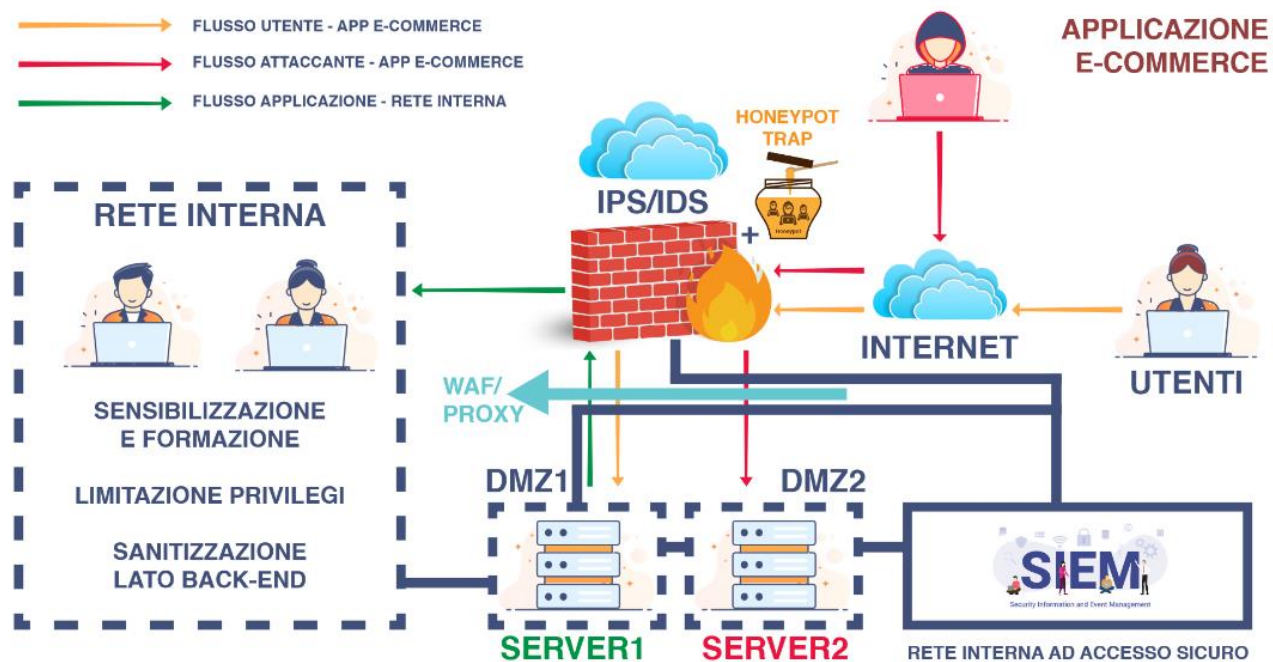
- **Purge:** Rimozione dei dati con metodi fisici, come l'utilizzo di magneti.
- **Destroy:** Distruzione totale del disco mediante alte temperature, disintegrazione, ecc.
- **Clear:** Rimozione dei dati con tecniche di factory reset o sovrascrittura del disco molte volte.



# DRAAS

è possibile ricorrere al **DRAAS (Disaster Recovery as a Service)**: i cloud provider mettono a disposizione delle aziende un'infrastruttura cloud che può essere attivata immediatamente in caso di disastro sul sito principale dell'azienda. Sebbene ci siano tempi di latenza nello switch dal sito primario a quello secondario, questa soluzione è conveniente poiché si paga solo quando si attinge al servizio in situazioni di emergenza. In questo modo, si trasferisce il rischio legato alla gestione dei disastri a un servizio esterno.

# Infrastruttura di rete proposta finale





# Grazie

MICHELE GARZONI ESAME MODULO 5