Traccia:

Esercizio Traccia e requisiti Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

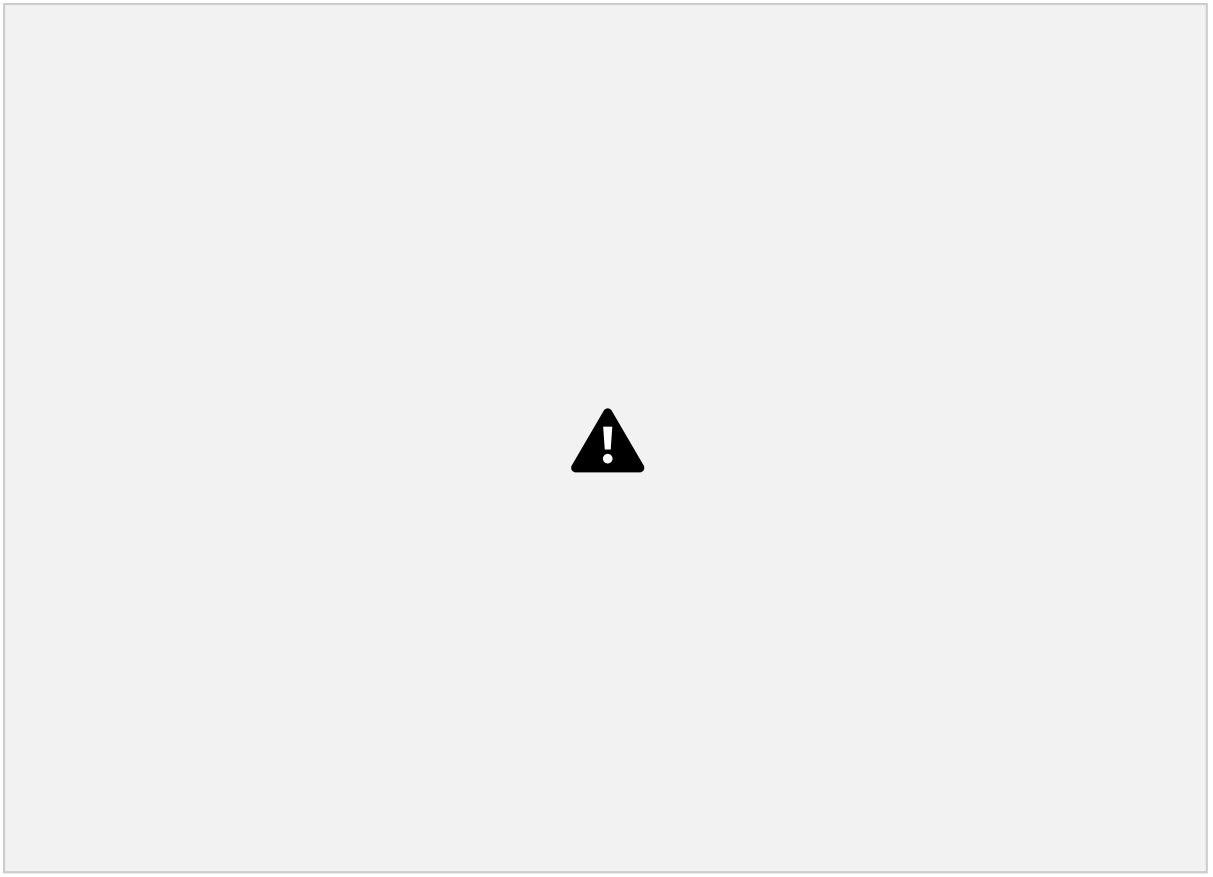
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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



PUNTO 1: Azioni preventive

1. Rafforzamento della rete:

Implementazione di un Web Application Firewall (WAF): un WAF funge da scudo per l'applicazione web, filtrando il traffico in ingresso e bloccando potenziali minacce. È fondamentale scegliere un WAF con funzionalità specifiche per la protezione da attacchi SQL injection e Cross-Site Scripting (XSS).

Configurazione di regole WAF: le regole WAF definiscono il comportamento del firewall in base a parametri come indirizzi IP, tipi di richieste e contenuti sospetti. È importante configurare correttamente le regole per garantire un'adeguata protezione senza bloccare accidentalmente traffico legittimo.

2. Sviluppo sicuro del software:

Adozione di un modello SDLC (Software Development Life Cycle): un SDLC definisce un processo strutturato per lo sviluppo del software, integrando pratiche di sicurezza in ogni fase. Due modelli comuni sono:

Modello a spirale: prevede un ciclo iterativo di sviluppo, con fasi di pianificazione, progettazione, implementazione, test e revisione. La sicurezza viene considerata in ogni fase, con test specifici per identificare e correggere vulnerabilità.

Modello agile: favorisce un approccio incrementale e adattivo, con rilasci frequenti di piccole porzioni di software. La sicurezza viene integrata nel processo tramite attività come code review, test di sicurezza automatizzati e formazione continua degli sviluppatori.

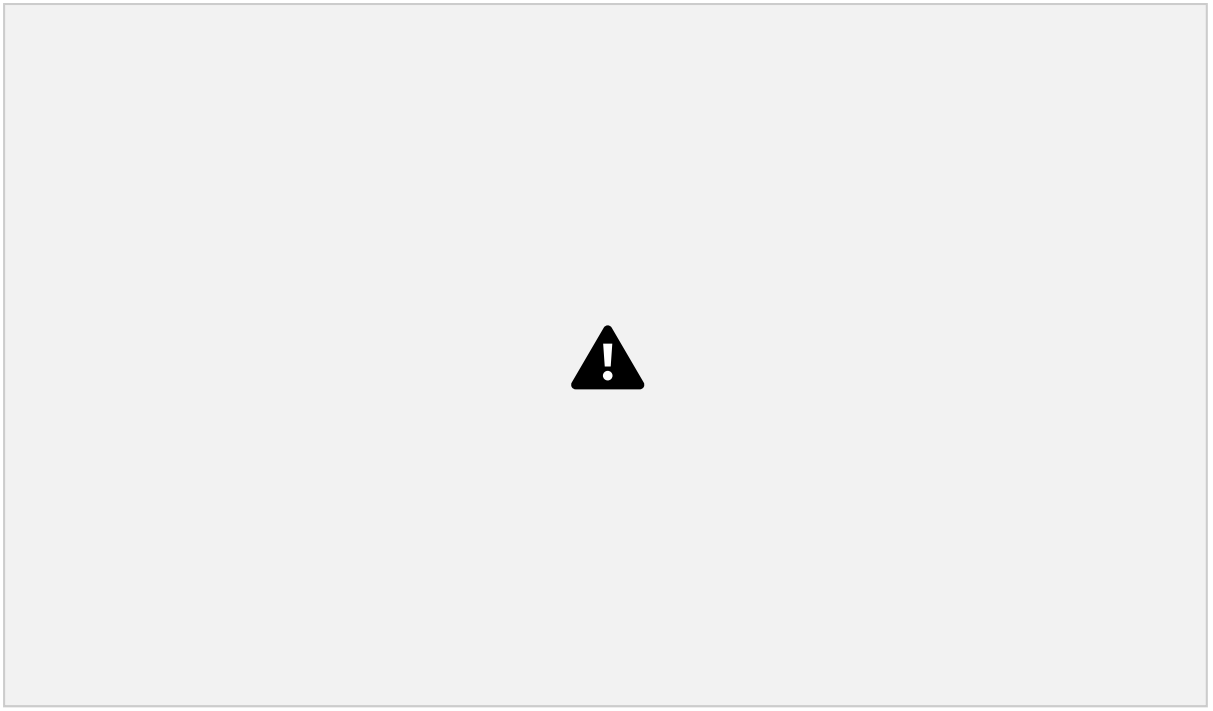
Integrazione del modello DevSecOps: DevSecOps unisce sviluppo (Dev) e sicurezza (SecOps) in un unico processo, promuovendo la collaborazione tra team di sviluppo e sicurezza fin dalle prime fasi del progetto. I test di sicurezza vengono integrati nel flusso di lavoro continuo, consentendo di identificare e correggere vulnerabilità in modo rapido ed efficiente.

L'implementazione di queste misure preventive può contribuire significativamente a:

Riduzione del rischio di attacchi: un WAF e un SDLC ben strutturato possono bloccare o mitigare la maggior parte degli attacchi comuni.

Protezione dei dati sensibili: prevenendo intrusioni e fughe di dati, si salvaguardano informazioni riservate e si tutela la reputazione dell'azienda.

Miglioramento della conformità normativa: molte normative, come il GDPR, richiedono l'implementazione di misure di sicurezza adeguate per la protezione dei dati.



PUNTO 2: Impatti sul business

In questo punto viene descritto un **attacco DDoS** che ha causato l'indisponibilità dell'applicazione web per 10 minuti, con un **costo stimato di 15.000€**. Non è possibile determinare la perdita annuale esatta a causa dell'incertezza sulla frequenza di tali eventi.

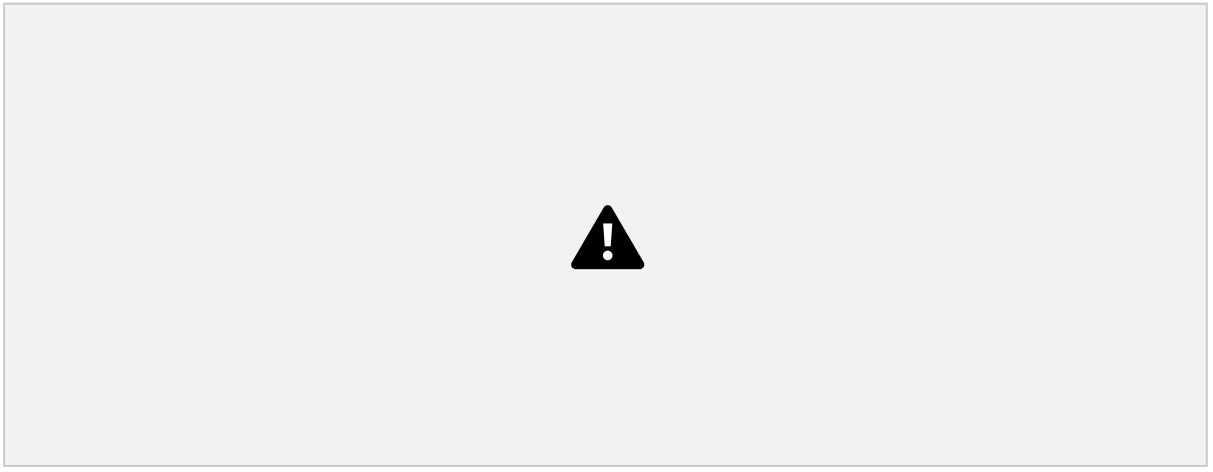
Per contrastare gli attacchi DDoS e garantire la continuità del servizio, viene proposta l'implementazione di una soluzione **DRaaS (Disaster Recovery as a Service)**. Questa soluzione offre i seguenti vantaggi:

Protezione dagli attacchi DDoS: il DRaaS garantisce la disponibilità di un'infrastruttura di backup in grado di gestire il traffico in caso di attacchi DDoS, minimizzando i tempi di inattività e le perdite economiche.

Costi prevedibili: il DRaaS prevede un canone mensile di 2044,00 $, che consente di pianificare e gestire le spese in modo efficace.

Ritorno sull'investimento (ROI): l'azienda stima che il DRaaS generi un ROI positivo dopo soli 30 minuti di indisponibilità causata da un attacco DDoS.

Scalabilità: la soluzione DRaaS può essere scalata per adattarsi alle esigenze aziendali, garantendo una protezione adeguata anche in caso di attacchi di grandi dimensioni.



Frequenza degli attacchi: la decisione di investire nel DRaaS si basa sulla plausibilità di ulteriori attacchi DDoS durante l'anno. Una valutazione accurata del rischio è fondamentale per determinare se il ROI giustifichi il costo.

Implementazione e gestione: l'implementazione e la gestione del DRaaS richiedono competenze tecniche specifiche. È importante valutare la disponibilità di risorse interne o la necessità di affidarsi a fornitori esterni.

Test e collaudo: è fondamentale testare regolarmente la soluzione DRaaS per garantire che funzioni correttamente in caso di disastro.

L'implementazione di una soluzione DRaaS rappresenta un'opzione valida per proteggere l'applicazione web da attacchi DDoS e garantire la continuità del servizio. La valutazione dell'investimento deve essere basata su una stima accurata del rischio, considerando i costi, i benefici e le risorse disponibili.

PUNTO 3: response

In questo punto, l'obiettivo non è la rimozione del malware che ha infettato l'applicazione, bensì iimpedirne la propagazione nella rete interna. Per questo scopo, viene proposta l'implementazione di una **soluzione di isolamento dell'incidente** e di una **configurazione di segmentazione preventiva della rete**.

Soluzione proposta:

1. **Isolamento dell'incidente:**

Implementare una soluzione di isolamento per separare il sistema infetto dal resto della rete interna. Questo può essere realizzato utilizzando:

VLAN (Virtual Local Area Network): creare una VLAN dedicata per il sistema infetto, isolandolo logicamente dal resto della rete.

Dispositivi di rete dedicati: utilizzare un router o uno switch separato per il sistema infetto, creando una rete fisica isolata.

Soluzioni di sicurezza basate su software: utilizzare software di sicurezza in grado di confinare il traffico infetto e impedire la sua comunicazione con altri sistemi.

2. **Segmentazione preventiva della rete:**

Segmentare la rete interna in diverse zone logiche o VLAN, raggruppando i sistemi in base a funzione, reparto o livello di sicurezza.

Implementare controlli di accesso granulari tra le diverse zone, consentendo solo il traffico necessario per il normale funzionamento.

Posizionare firewall all'interno delle zone per filtrare il traffico e bloccare le minacce.

Posizionamento del dispositivo di routing:

Il dispositivo di routing (o la soluzione che gestisce sia il routing che l'isolamento) dovrebbe essere posizionato **a valle del firewall principale**. Questo garantisce che il firewall possa filtrare il traffico in ingresso e proteggere la rete interna da minacce esterne.

Le due strutture (sistema infetto e rete interna) dovrebbero trovarsi su **sottoreti diverse** per evitare connessioni dirette e facilitare l'isolamento.

Questa soluzione consente di contenere il malware e impedire la sua diffusione nella rete interna, minimizzando i danni e facilitando la bonifica.

La segmentazione preventiva della rete riduce la superficie di attacco e migliora la postura di sicurezza generale dell'organizzazione.

La scelta della soluzione di isolamento e della configurazione di segmentazione dipende dalle specifiche esigenze e dall'architettura della rete.

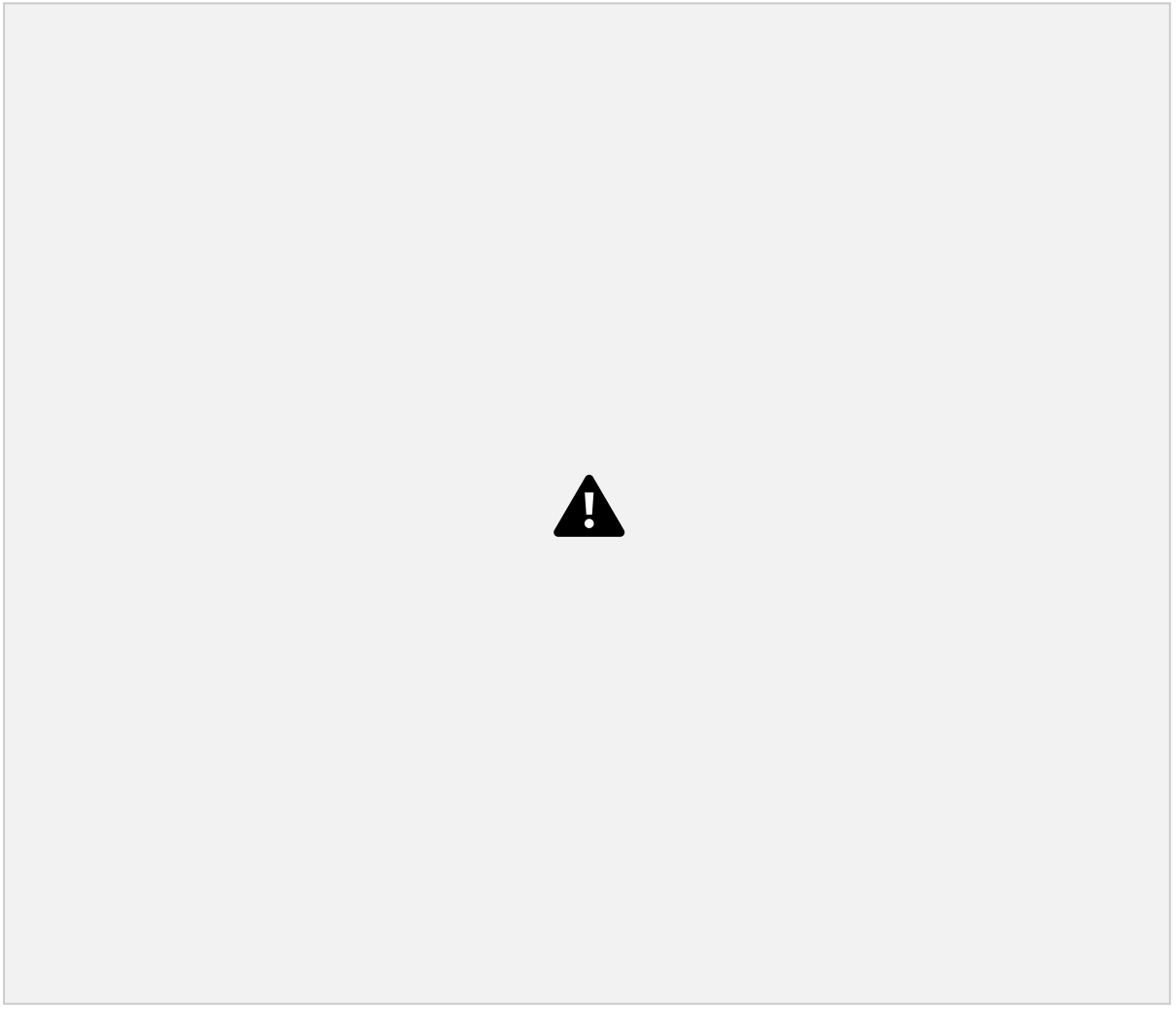
È importante pianificare attentamente l'implementazione per evitare interruzioni del servizio e garantire una corretta comunicazione tra le diverse zone di rete.

La segmentazione richiede la gestione attenta delle regole di accesso e dei firewall per garantire il corretto funzionamento delle applicazioni e dei servizi.

L'isolamento dell'incidente e la segmentazione preventiva della rete rappresentano strategie efficaci per contenere i danni da attacchi malware e proteggere la rete interna. L'implementazione di queste misure richiede una valutazione accurata delle esigenze e delle risorse dell'organizzazione, nonché una pianificazione attenta e una corretta configurazione.

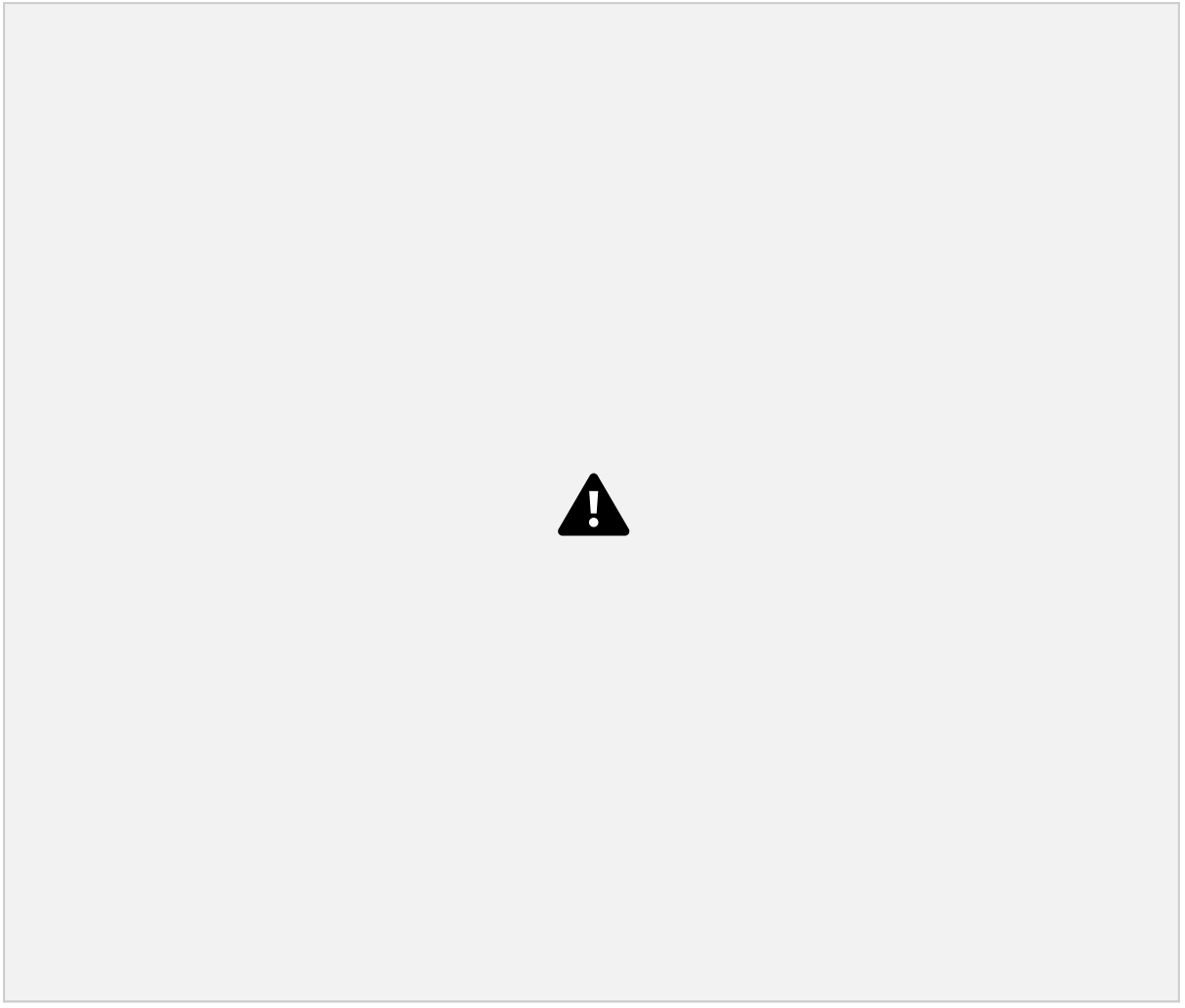
Oltre alle misure descritte, è importante implementare pratiche di sicurezza di base come aggiornamenti software regolari, backup regolari e formazione sulla sicurezza per gli utenti.

È consigliabile avvalersi di esperti di sicurezza informatica per la valutazione del rischio, la scelta delle soluzioni di sicurezza e l'implementazione delle misure di protezione.



PUNTO numero 4 :Soluzione completa

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



PUNTO 5: Modifica aggressiva, migrazione sul cloud

Il punto 5 richiede una riprogettazione radicale dell'infrastruttura, spostando il servizio e-commerce verso il cloud.

Sebbene l'azienda sia di medie dimensioni con un costo elevato per minuto di downtime (€ 1.500), non rientra nella categoria delle grandi aziende con esigenze di massima riservatezza (segreti militari, governativi, brevetti).

Trattandosi di e-commerce, la riservatezza dei dati non è paragonabile a settori più sensibili.

Proposta:

Spostamento del rischio: Migrare la parte di rete che espone il servizio e-commerce verso il cloud, adottando una strategia di "spostamento del rischio".

Vantaggi:

Maggiore sicurezza: I provider cloud offrono infrastrutture altamente sicure e gestite da professionisti, con tecnologie avanzate per la protezione da attacchi e intrusioni.

Scalabilità: Il cloud offre la possibilità di scalare l'infrastruttura in modo rapido ed elastico in base alle esigenze del business, senza dover investire in hardware e software aggiuntivi.

Riduzioni di costo: A lungo termine, il cloud può comportare un risparmio sui costi di gestione dell'infrastruttura IT, liberando risorse per investire in altri ambiti strategici.

Architettura proposta:

Rete privata: Mantenere una rete privata on-premises per la gestione interna dell'azienda (relazioni con clienti e fornitori, sviluppo software, etc.).

Cloud: Spostare la parte di erogazione del servizio e-commerce su una piattaforma cloud (AWS, Microsoft Azure, etc.).

Responsabilità:

Azienda: Responsabile della gestione del software e-commerce, garantendone il miglioramento continuo e l'applicazione di patch di sicurezza bimestrali.

Fornitore cloud: Responsabile della gestione dell'infrastruttura cloud, garantendone la sicurezza, la disponibilità e l'affidabilità.

Valutazioni periodiche: Il fornitore cloud eseguirà bimestralmente valutazioni della sicurezza per identificare e mitigare potenziali vulnerabilità.

La migrazione verso il cloud del servizio e-commerce rappresenta un'opzione strategica per migliorare la sicurezza, la scalabilità e l'efficienza dell'infrastruttura IT, favorendo la crescita e l'innovazione del business. La scelta del fornitore cloud e la configurazione dei servizi devono essere effettuate con attenzione, valutando le specifiche esigenze e gli obiettivi dell'azienda.

È importante valutare attentamente i costi associati alla migrazione e al mantenimento del servizio cloud, confrontandoli con i costi dell'infrastruttura on-premises esistente.

La migrazione al cloud richiede una pianificazione accurata e una collaborazione efficace tra l'azienda e il fornitore cloud per garantire un processo fluido e minimizzare i tempi di inattività.

È fondamentale adottare le migliori pratiche di sicurezza per proteggere i dati e le applicazioni nel cloud, seguendo le linee guida e le raccomandazioni del fornitore cloud scelto.