M5 - Progetto Finale - Modifica Aggressiva

Budget Disponibile: 20.000 € - 30.000 €

Considerando il budget di 20.000 € - 30.000 € e l'obiettivo di una "modifica più aggressiva" che integri anche la soluzione al punto 2 (mitigazione DDoS), la strategia si concentrerà sull'adozione di servizi gestiti e sulla resilienza, piuttosto che sull'acquisto massivo di hardware on-premise, che supererebbe il budget.

Le modifiche aggressive mirano a spostare parte del carico di sicurezza e disponibilità su fornitori specializzati e a rendere l'infrastruttura più elastica e difficile da attaccare/compromettere.

Soluzioni Proposte con Stima di Costo (Budget: 20-30k €/anno stimato):

1. Adozione di un Servizio di Protezione DDoS e CDN Basato su Cloud (Priorità Alta):
    - Descrizione: Questo è l'investimento più significativo e cruciale per affrontare gli attacchi DDoS (punto 2). Un servizio come Cloudflare Enterprise (o un piano equivalente da Akamai, AWS Shield Advanced, Google Cloud Armor) offre protezione DDoS a tutti i livelli (network, transport, application), un Web Application Firewall (WAF) integrato (rafforzando il punto 1) e funzionalità di Content Delivery Network (CDN) per migliorare performance e resilienza. Le CDN distribuiscono i contenuti statici su edge server globali, riducendo il carico sui server di origine e rendendo il sito più veloce e resistente ai picchi di traffico.
    - Funzionalità aggressive: Non solo blocca DDoS, ma opera come un reverse proxy intelligente, nascondendo l'IP reale del server, offrendo caching (CDN) e protezioni WAF avanzate contro un'ampia gamma di attacchi, inclusi zero-day. La sua capacità di assorbire attacchi massivi è incomparabile con soluzioni on-premise di pari costo.
    - Stima costo: I piani Enterprise di questi servizi possono variare notevolmente, ma per un'applicazione e-commerce di medie dimensioni, si possono stimare costi nell'intervallo di 1.500 € - 3.000 €/mese (18.000 € - 36.000 €/anno). Un budget di 20-30k €/anno rientra in un piano robusto, sebbene possa essere al limite superiore o richiedere un'attenta selezione delle funzionalità. Questo investimento coprirebbe un aspetto critico della modifica "aggressiva" e risolverebbe direttamente il problema del DDoS.

2. Implementazione di EDR (Endpoint Detection and Response) / XDR (Extended Detection and Response) sull'Applicazione di E-commerce (Punto 3 - Response migliorata):
    - Descrizione: Sebbene la priorità fosse il contenimento della propagazione, una modifica aggressiva includerebbe una migliore visibilità e capacità di risposta sulla macchina infetta. Un EDR o XDR fornisce monitoraggio continuo, rilevamento avanzato delle minacce (anche sconosciute), analisi forense e capacità di risposta automatizzate sull'endpoint (server dell'applicazione).
    - Funzionalità aggressive: Va oltre un semplice antivirus, rilevando attività anomale, tentativi di movimento laterale del malware anche all'interno della stessa macchina (o verso altri componenti se le regole firewall sono permissive), e fornendo dati vitali per la remediation e la comprensione dell'attacco. Permette un'azione più proattiva nella bonifica della macchina, anche se la priorità immediata è il contenimento.
    - Stima costo: Per un singolo server critico, una soluzione EDR/XDR può costare da 50 € a 200 €/mese (600 € - 2.400 €/anno). Questo rientra ampiamente nel budget e offre un enorme valore aggiunto nella fase di risposta e bonifica.

3. Servizi di Sicurezza Gestiti (MSSP - Managed Security Service Provider) per Monitoraggio 24/7:
    - Descrizione: Con il budget rimasto, si potrebbe considerare di investire in un servizio MSSP per un monitoraggio di base 24/7 degli alert critici provenienti dal WAF/DDoS Protection e dall'EDR. Non si tratterebbe di un SOC completo, ma di un servizio di alerting e analisi di primo livello.
    - Funzionalità aggressive: Avere occhi esperti sulla sicurezza 24/7 riduce significativamente i tempi di rilevamento e risposta, specialmente per un'azienda che potrebbe non avere un team di sicurezza dedicato full-time.
    - Stima costo: Un servizio di monitoraggio entry-level o per un numero limitato di alert/dispositivi può costare da 500 € a 1.500 €/mese (6.000 € - 18.000 €/anno). Questo potrebbe spingere il budget al limite superiore se combinato con un piano DDoS Enterprise, ma è una modifica "aggressiva" per la prontezza di risposta.

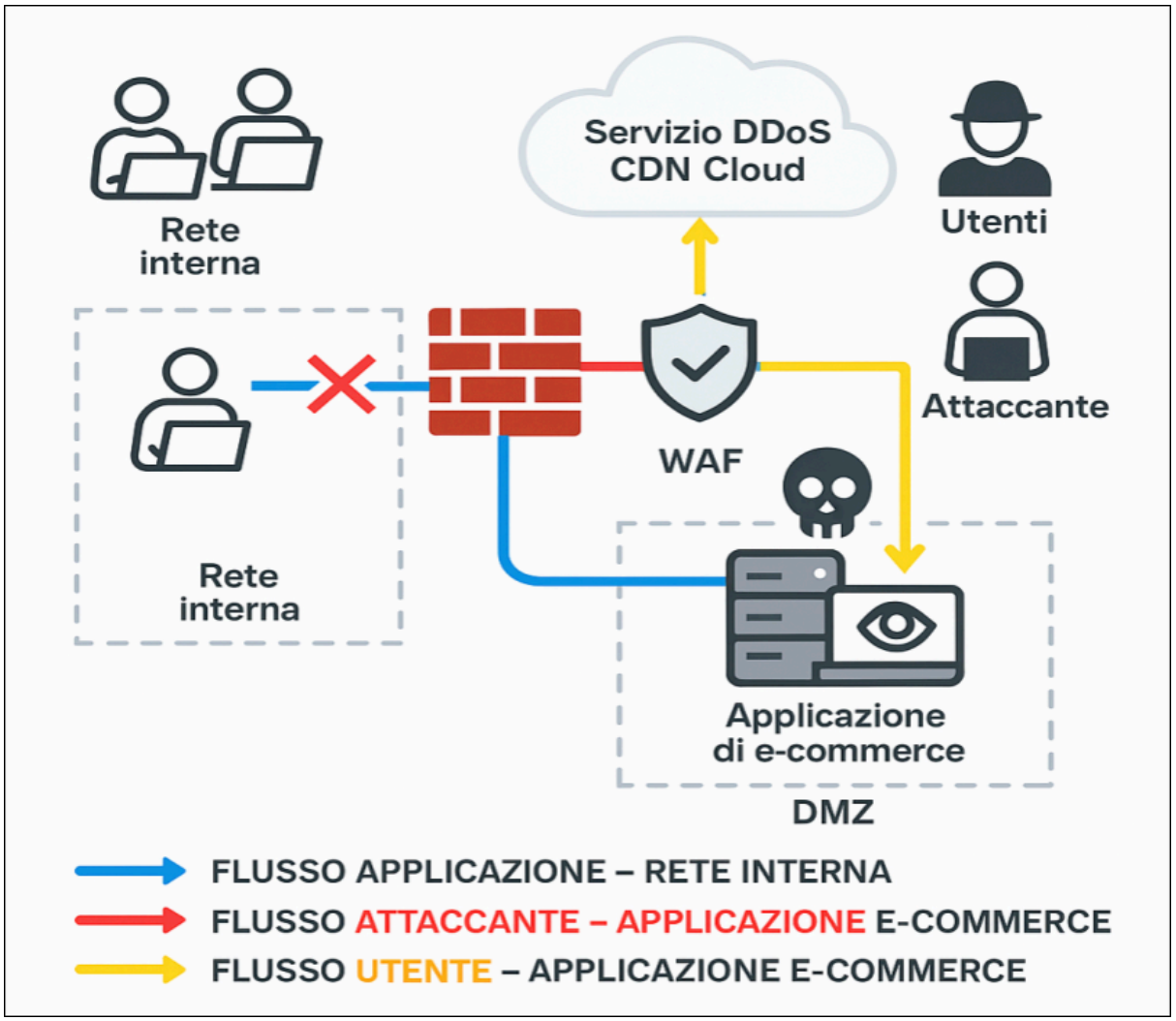
Riepilogo Allocazione Budget

1. Servizio DDoS/CDN Cloud (Enterprise): 20.000 € - 25.000 €
2. EDR per server applicazione: 1.000 € - 2.000 €
3. Margine/MSSP base: 0 € - 9.000 € (a seconda della scelta del piano DDoS/CDN)

Questa allocazione permetterebbe di coprire le minacce più impattanti (DDoS, SQLi/XSS, malware) con soluzioni di livello Enterprise, migliorando drasticamente la resilienza e la capacità di risposta.

Rappresentazione Architetturale della Modifica Aggressiva

La seguente figura illustra l'architettura di rete con le modifiche più aggressive implementate, focalizzandosi sull'integrazione di servizi di protezione DDoS/CDN basati su cloud e la presenza di un sistema EDR/XDR, oltre alle misure preventive e di risposta già discusse.



Conclusioni

Una modifica "aggressiva" dell'infrastruttura, con un budget di 20-30k €, si concentra sull'adozione di soluzioni basate su cloud per la protezione DDoS e CDN, che offrono scalabilità e resilienza impareggiabili contro attacchi voluminosi e applicativi. L'integrazione di un sistema EDR/XDR fornisce una visibilità e una capacità di risposta granulare direttamente sull'endpoint, rafforzando la gestione delle infezioni malware. Sebbene il budget possa essere stretto per servizi MSSP completi, un'allocazione intelligente permette di acquisire difese di livello enterprise contro le minacce più critiche, trasformando l'infrastruttura in un ambiente notevolmente più resiliente, proattivo e difficile da compromettere rispetto alla configurazione iniziale. Questo approccio garantisce un'ottima resa dell'investimento in termini di sicurezza e continuità del business.