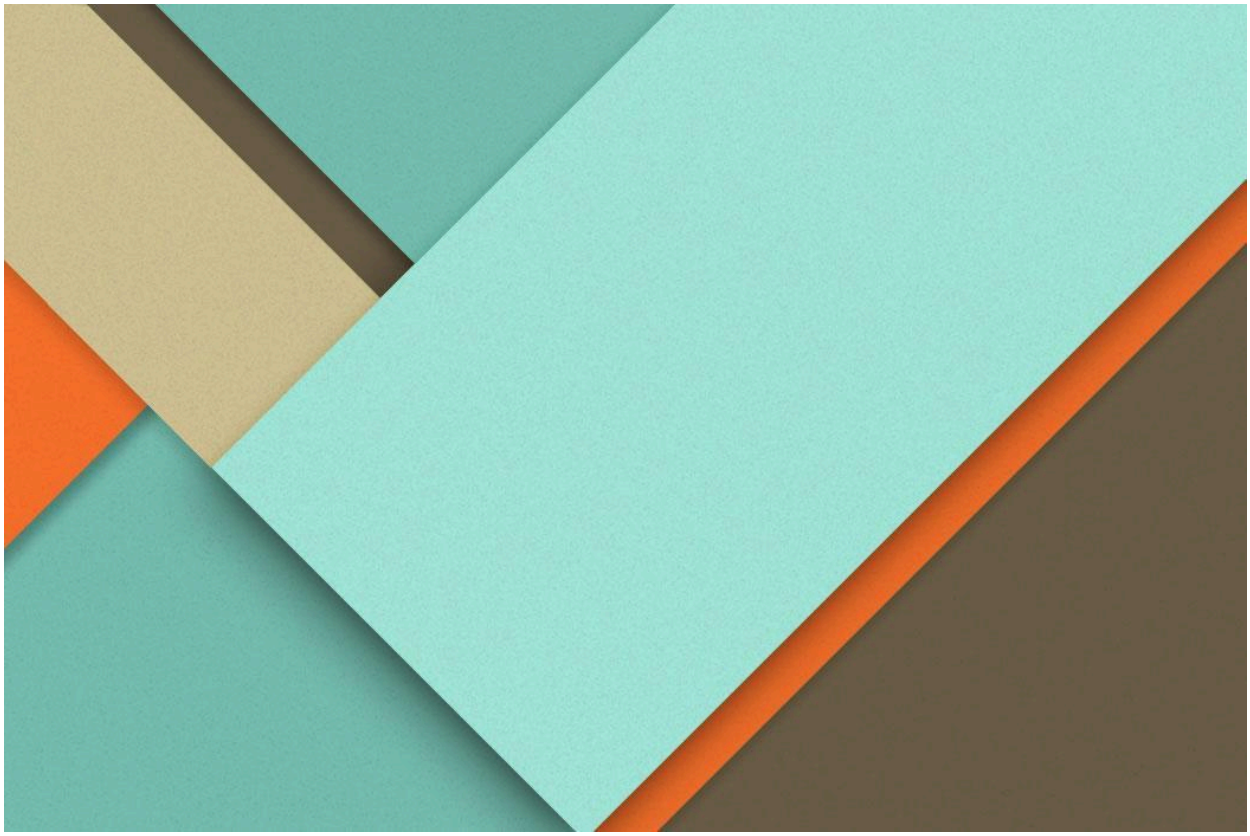

Progetto M5

25/03/2024

Rebecca Caldarella

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)

Svolgimento

1. Azioni preventive

Per difendere le applicazioni Web da attacchi di tipo SQLi oppure XSS è necessario implementare il Web Application Firewall (WAF). L'architettura di rete risultante è mostrata in figura 1.

2. Impatti sul business

Gli attacchi DoS hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, come potrebbe essere un'applicazione o un sito web.

Se l'applicazione Web subisse un attacco DDoS, rendendo i servizi inaccessibili per 10 minuti, considerando che in media gli utenti spendono €1.500 al minuto si avrebbe un impatto sul business pari a €15.000.

Al fine di proteggere la DMZ, si potrebbe aggiungere all'architettura precedente (che utilizza WAF) un Network Access Control (NAC), il quale permette di controllare gli accessi alla rete e quindi di limitare il numero di richieste eseguite.

Inoltre alla base di queste due tecnologie potrebbe essere integrato un IPS/IDS per tenere monitorato il traffico ed eventualmente gli attacchi in corso.

3. Response

Supponendo che sia stata rispettata la triade CIA, per assicurare l'availability (la disponibilità del dato) è stato precedentemente effettuato un backup dell'applicazione web che possa essere utilizzato in caso di necessità.

In questo caso, essendo l'app infetta da malware, viene indirizzato tutto il traffico degli utenti autorizzati verso il backup dell'applicazione, mentre gli utenti non autorizzati (come l'hacker in questione) continueranno ad essere indirizzati verso l'app infetta. (Figura 3)

4. Figura 4

5. Modifica più aggressiva dell'infrastruttura

Vengono aggiunti tra le azioni preventive i sistemi di prevenzione e rilevamento delle intrusioni (IPS/IDS, Intrusion Detection System e Intrusion Prevention System), in modo tale da individuare preventivamente i potenziali attacchi. Il sistema di

rilevamento si occupa solo del monitoraggio di determinati eventi di sicurezza in tempo reale, mentre il sistema di prevenzione supporta anche delle azioni automatiche per fermare la potenziale intrusione.

Inoltre è stato implementato un firewall dedicato alla rete interna per isolarlo ancora di più rispetto alla DNZ.

Per aumentare ulteriormente la sicurezza si può ammettere l'utilizzo di una rete di quarantena nella rete interna. (Figura 5)