

Progetto

Settimana 9

Lezione 5

Francesco Alfonsi

Indice

Traccia e architettura di rete.....3

Azioni Preventive

- ✓ Iniezione SQL e attacchi XSS: impatti sulle applicazioni web.....4
- ✓ Comprendere DMZ, Web Application Firewall (WAF) e Intranet.....5
- ✓ Presentazione nuova architettura di rete.....6

Impatto sul business

- ✓ Attacchi di tipo DDoS: cosa sono e quale impatto possono avere sul business.....7
- ✓ Proteggere l'attività dagli attacchi DDoS: prevenzione.....8
- ✓ Calcolo dell'impatto sul business.....9

Response

- ✓ Malware, infezione in DMZ e strategia di risposta.....10
- ✓ Modifica dello schema di rete con la soluzione proposta.....11

Traccia

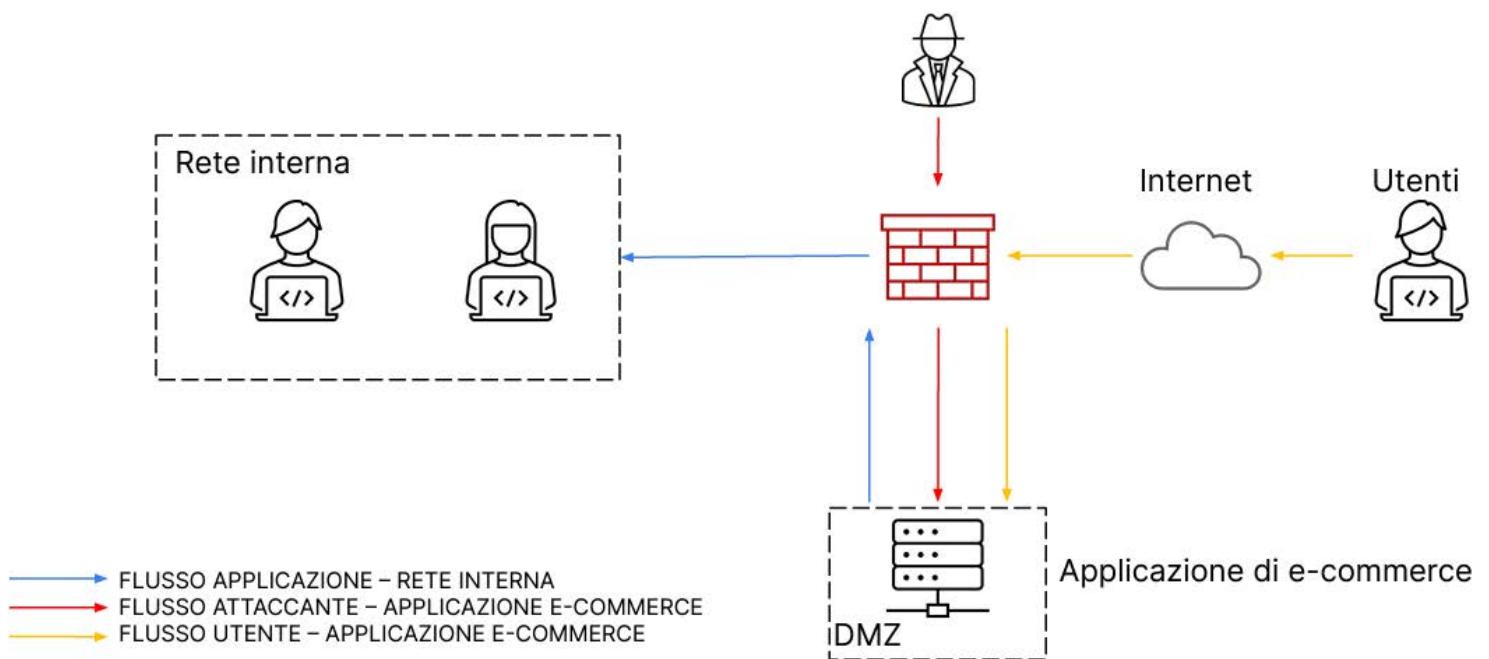
Con riferimento alla figura sottostante, rispondere ai seguenti quesiti.

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.

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 sottostante con la soluzione proposta.

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

Prima di vedere come migliorare la sicurezza dell'infrastruttura di rete attuale, capiamo come funzionano gli attacchi di tipo SQL injection e XSS sulle applicazioni web, quali danni, qualitativi e quantitativi, possono portare all'azienda e quali azioni preventive possono essere utilizzate per contrastarli. Capiamo inoltre, come funzionano le DMZ, le reti interne e i Web Application Firewall, per comprendere perché l'inserimento di quest'ultimo all'interno della configurazione di rete con la quale stiamo lavorando sia un'azione preventiva che porterà benefici per la sicurezza dell'azienda.

Iniezione SQL e attacchi XSS: impatti sulle applicazioni web

Sia gli attacchi di iniezione SQL (SQLi) che quelli di cross-site scripting (XSS) possono avere gravi conseguenze per le applicazioni web, compromettendo:

Dati

SQLi: Gli attaccanti possono rubare dati sensibili come nomi utente, password, numeri di carte di credito e informazioni personali memorizzate nel database.

XSS: Gli attaccanti possono iniettare script dannosi nel sito web, potenzialmente rubando i dati degli utenti inseriti nei moduli o nei cookie.

Funzionalità

SQLi: Gli attaccanti possono modificare o eliminare i dati nel database, portando a informazioni corrotte e potenziali crash.

XSS: Gli attaccanti possono controllare parti del comportamento del sito web, reindirizzando gli utenti verso siti dannosi, modificando i contenuti o persino lanciando ulteriori attacchi.

Reputazione

Entrambi: Attacchi riusciti possono danneggiare la reputazione dell'azienda, portando a perdita di fiducia, abbandono degli utenti e potenziali conseguenze legali.

Impatti aggiuntivi

SEO: I contenuti iniettati possono influire sul posizionamento nei motori di ricerca.

Attacchi DDoS: Le credenziali rubate possono essere utilizzate in ulteriori attacchi.

Prevenzione

Sanificare gli input: Validare e sanificare tutti gli input degli utenti prima di elaborarli.

Usare dichiarazioni preparate: Non incorporare direttamente l'input dell'utente nelle query SQL.

Codificare l'output: Codificare correttamente i dati visualizzati sul sito web per prevenire l'iniezione di script.

Tenere aggiornato il software: Applicare prontamente le patch di sicurezza per risolvere le vulnerabilità.

Comprendendo questi impatti e adottando misure pro-attive, si possono ridurre significativamente i rischi di attacchi SQLi e XSS e proteggere l'applicazione web e i suoi utenti.

Comprendere DMZ, Web Application Firewall (WAF) e Intranet

DMZ (zona demilitarizzata)

Una DMZ può essere vista come una zona buffer tra la rete interna affidabile (intranet) e l'Internet pubblica non affidabile. Si tratta di un segmento di rete separato che ospita risorse accessibili pubblicamente, come server Web e server di posta elettronica, mantenendo al sicuro i dati interni sensibili. Si consideri come un punto di ingresso controllato per le interazioni esterne.

Firewall per applicazioni Web (WAF)

Si pensi a un WAF come a una guardia di sicurezza per le applicazioni web che risiedono nella DMZ. Si trova tra Internet e i server web, e si occupa dell'ispezione di tutto il traffico in entrata per individuare contenuti e attività dannose. Filtra le richieste dannose, come SQL injection o tentativi di cross-site scripting (XSS), prima che raggiungano le applicazioni.

Intranet

L'intranet è la rete privata e affidabile all'interno di un'organizzazione. Ospita dati sensibili, risorse interne e applicazioni utilizzate dai dipendenti e dal personale autorizzato. Questa rete è completamente isolata da Internet e dalla DMZ, accessibile solo tramite metodi di autenticazione sicuri.

Come lavorano insieme

- i. **Traffico esterno:** quando qualcuno accede al sito web da Internet, la sua richiesta passa prima attraverso il WAF. Il WAF analizza la richiesta e blocca qualsiasi attività sospetta o codice dannoso.
- ii. **Traffico pulito:** se la richiesta è ritenuta sicura, il WAF la inoltra al server web appropriato nella DMZ.
- iii. **Risorse interne:** il server web elabora la richiesta e genera una risposta.
- iv. **Comunicazione sicura:** la risposta ritorna quindi attraverso il WAF e arriva su Internet.
- v. **Accesso alla Intranet:** i dipendenti dell'organizzazione accedono alle risorse interne direttamente tramite la Intranet utilizzando accessi sicuri. Non hanno accesso diretto alla DMZ o a Internet.

Vantaggi di questa configurazione

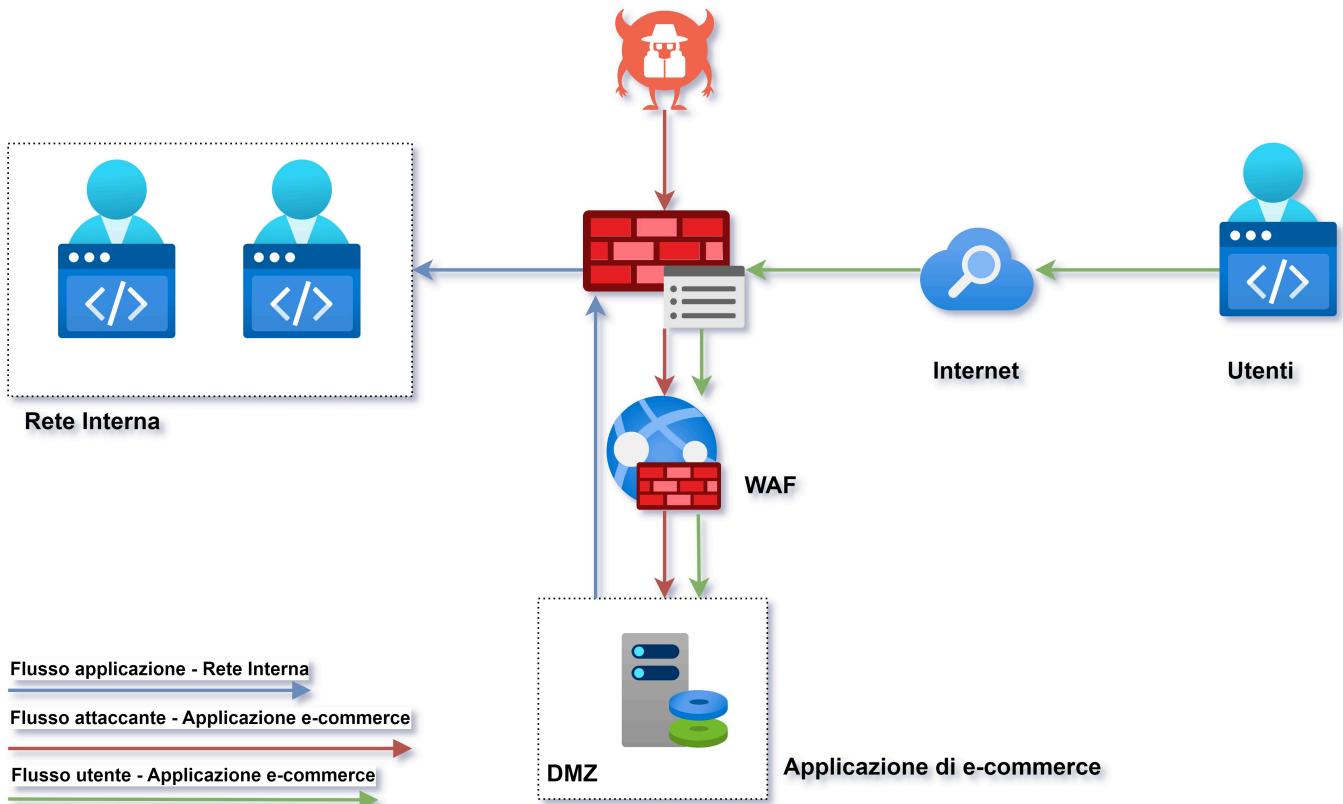
- **Sicurezza migliorata:** la DMZ isola i dati sensibili da Internet, mentre il WAF filtra gli attacchi dannosi prima che raggiungano le applicazioni.
- **Prestazioni migliorate:** la DMZ riduce il carico sulla rete interna e migliora le prestazioni delle applicazioni web.
- **Maggiore controllo:** si ha un maggiore controllo su quali risorse sono accessibili da Internet e su come gli utenti vi accedono.

Note aggiuntive

Anche altre misure di sicurezza, come i sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS) e pratiche di codifica sicura, sono importanti per una protezione completa.

Presentazione nuova architettura di rete

Per le motivazioni viste nelle pagine precedenti, si consiglia quindi l'adozione di un WAF che si posiziona tra la DMZ e la rete internet, in modo da proteggere il traffico in entrata sull'applicazione web. Di seguito la nuova architettura di rete proposta con l'implementazione di tale strumento.



IMPATTO SUL BUSINESS

Attacchi di tipo DDoS: cosa sono e quale impatto possono avere sul business

Un attacco Distributed Denial-of-Service (DDoS) è un tentativo malevolo di sopraffare un sito web o un servizio online con un flusso enorme di traffico internet, rendendolo inaccessibile agli utenti legittimi. In un attacco DDoS, ci sono milioni di dispositivi compromessi, detti anche bot, controllati dall'attaccante, che inondano il server target di richieste fasulle, consumando larghezza di banda e impedendo agli utenti di accedere ai servizi.

Tipi di attacchi DDoS

Attacchi volumetrici: Inondano il server con un'elevata quantità di dati, sovraccaricando la larghezza di banda e causando interruzioni.

Attacchi di protocollo: Sfruttano vulnerabilità nei protocolli di rete per interrompere la comunicazione e bloccare i server.

Attacchi a livello di applicazione: Prendono di mira parti specifiche dell'applicazione, sovraccaricando risorse e causando rallentamenti o blocchi.

Gli attacchi DDoS possono avere un impatto devastante sulle attività in diversi modi

Perdite finanziarie: Le interruzioni causate dagli attacchi DDoS possono comportare perdite di vendite, entrate e produttività.

Danno alla reputazione: Il downtime può danneggiare l'immagine del marchio e la fiducia dei clienti.

Interruzione operativa: Gli attacchi possono interrompere le operazioni interne, le comunicazioni e la produttività dei dipendenti.

Costi di sicurezza: Mitigare e riprendersi dagli attacchi DDoS può essere costoso, richiedendo investimenti aggiuntivi in sicurezza.

Proteggere l'attività dagli attacchi DDoS: prevenzione

Proteggere l'azienda dagli attacchi DDoS richiede un approccio multi livello che combina soluzioni tecniche, preparazione organizzativa e consapevolezza dei dipendenti. Di seguito una suddivisione delle principali attività di prevenzione:

Rete e infrastruttura

Investire in una connessione internet ad alta larghezza di banda: una connessione internet robusta può gestire meglio i volumi di traffico aumentati durante un attacco.

Utilizzare una Content Delivery Network (CDN): le CDN distribuiscono il contenuto su più server a livello globale, rendendo più difficile per gli aggressori sovraccaricare un singolo punto.

Implementare servizi di mitigazione DDoS: questi servizi offrono rilevamento e filtraggio in tempo reale del traffico dannoso, spesso utilizzando tecniche come il filtraggio IP, l'analisi del traffico e il rilevamento di bot.

Aggiornare regolarmente il software e il firmware di sistema: l'applicazione di patch chiude rapidamente i potenziali punti di accesso per gli aggressori.

Segmentare la rete: creare reti separate per i sistemi critici e i servizi rivolti al pubblico limita la superficie di attacco.

Monitorare i modelli di traffico di rete: identificare le deviazioni dai livelli di traffico normali, che potrebbero indicare un attacco.

Preparazione organizzativa

Sviluppare un piano di risposta agli incidenti DDoS: questo piano dovrebbe delineare i ruoli, le responsabilità, i protocolli di comunicazione e le procedure di mitigazione per diversi scenari di attacco.

Condurre regolarmente esercitazioni e simulazioni: testare il piano di risposta agli incidenti per assicurarsi che tutti conoscano i propri ruoli e le procedure.

Mantenere chiari canali di comunicazione: stabilire protocolli di comunicazione per informare le principali parti interessate durante un attacco.

Sviluppare piani di backup e ripristino: assicurarsi di avere backup di dati e sistemi critici per facilitare un rapido ripristino dopo un attacco.

Consapevolezza dei dipendenti

Formazione dei dipendenti su phishing e truffe di ingegneria sociale: queste tecniche sono spesso utilizzate per accedere a dispositivi o reti utilizzati negli attacchi DDoS.

Enfasi su password sicure e autenticazione a due fattori: incoraggiare i dipendenti a utilizzare password solide e univoche e ad abilitare l'autenticazione a due fattori per gli account critici.

Insegnare ai dipendenti i segni di un attacco DDoS: addestrare a riconoscere attività di rete insolite o rallentamenti del sistema e a segnalarli immediatamente.

Calcolo dell'impatto sul business

Approccio quantitativo

Sappiamo che, di media, attraverso l'applicazione web, l'azienda incassa €1.500,00 ogni minuto. Statisticamente parlando, un errore di sistema che ne causi il mancato funzionamento per un tempo stimato di 10 minuti, influirebbe, potenzialmente, per un importo pari a circa €15.000,00 - ovvero il semplice prodotto del tempo espresso in minuti per il guadagno stimato al minuto. L'incidente rientrerebbe quindi tra quelli di criticità media - impatto economico non indifferente, tra i 10.000,00 e i 500.000,00 euro).

Approccio qualitativo

Tuttavia, come abbiamo avuto modo di approfondire precedentemente, il mero calcolo della perdita basato sull'incasso medio nell'intervallo di tempo, è un approccio superficiale che può dare soltanto una stima immediata e dal basso danno arrecato. Se volessimo fornire un quadro più completo della potenziale perdita da parte della società, dovremmo considerare anche quello che viene definito *impatto di tipo qualitativo*. Si pensi alla cattiva pubblicità che verrebbe a colpire l'azienda, o alla sfiducia che il disservizio causerebbe nei clienti; tutti fattori, questi, che potrebbero non avere evidenze nell'immediato, ma farsi sentire nel lungo termine.

Response

Malware, infezione in DMZ e strategia di risposta

Comprendere il malware

Il malware è un software progettato per danneggiare un sistema informatico. Può rubare dati, crittografare file, interrompere le operazioni o addirittura prendere il controllo del sistema. Esistono molti tipi diversi di malware, tra cui virus, worm, Trojan, ransomware e spyware.

Infezione in una DMZ

Sebbene la DMZ aggiunga un livello di sicurezza, le applicazioni web al suo interno possono comunque essere vulnerabili all'infezione da malware. Alcuni metodi di infezione comuni includono:

Sfruttamento di vulnerabilità: Gli aggressori possono sfruttare vulnerabilità non patchate nel software dell'applicazione web o nel sistema operativo sottostante.

Social Engineering: Si possono indurre gli utenti a scaricare file infetti o a cliccare su link dannosi.

Attacchi alla catena di fornitura: Si possono compromettere software o servizi di terze parti utilizzati dall'applicazione web.

Strategia di risposta

Isolamento della macchina infetta: Questo è un primo passo fondamentale per prevenire la diffusione del malware. Nel nostro scenario, isolare la macchina all'interno della DMZ dall'intranet è l'approccio più logico, utile anche per studiare, nel frattempo, come si sviluppa l'attacco, così da comprendere quali misure di sicurezza possono essere adottate in una successiva fase di prevenzione.

Identificazione del malware: Si analizza quindi la macchina infetta per determinare il tipo specifico di malware e la sua funzionalità.

Contenimento del danno: Si valuta l'impatto dell'infezione e si adottano misure per prevenirne ulteriori, come il blocco della crittografia dei file o l'esfiltrazione dei dati.

Raccolta di prove: Si possono analizzare i log e le configurazioni di sistema per comprendere le azioni dell'aggressore e raccogliere prove per potenziali azioni legali o futuri miglioramenti della sicurezza.

Eliminazione del malware: Una volta che si ha una chiara comprensione dell'infezione, si può sviluppare un piano per rimuovere completamente il malware. Ciò potrebbe comportare l'utilizzo di software anti-malware specializzato, l'applicazione di patch alle vulnerabilità o la re-installazione del sistema operativo.

Ripristino dall'attacco: La fase finale, successiva all'eliminazione del malware, è quella del ripristino dei dati e delle funzionalità perdute; è importante, inoltre, affrontare tutte le vulnerabilità sottostanti per prevenire future infezioni.

Modifica dello schema di rete con la soluzione proposta

