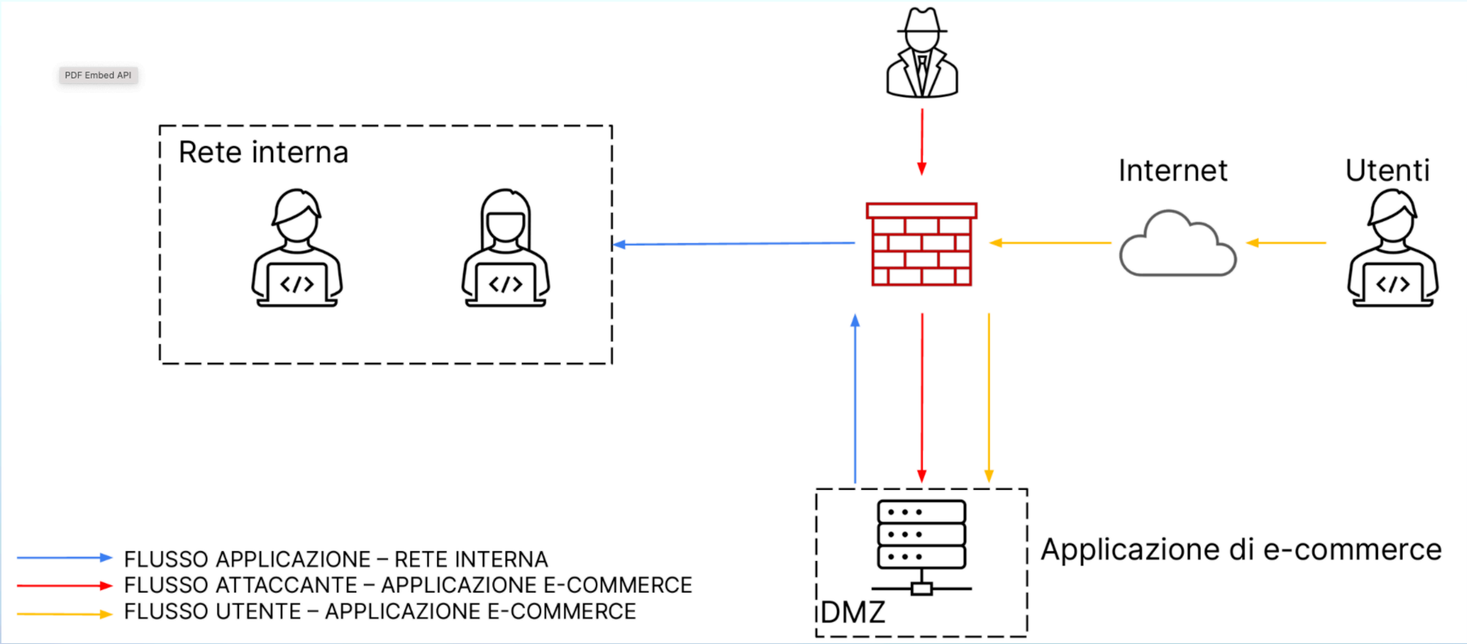
Cyber Security & Ethical Hacking

Prevenzione e risoluzione di casistica aziendale.

Vincenzo Colletta 24/11/2023

Introduzione

Nella traccia odierna ci viene richiesto di modificare un diagramma fornitoci, che rappresenta una possibile configurazione di una rete aziendale. Azioni preventive, impatti sul business e response, saranno i nostri obiettivi.



Introduzione

Approfondimento Tasks.

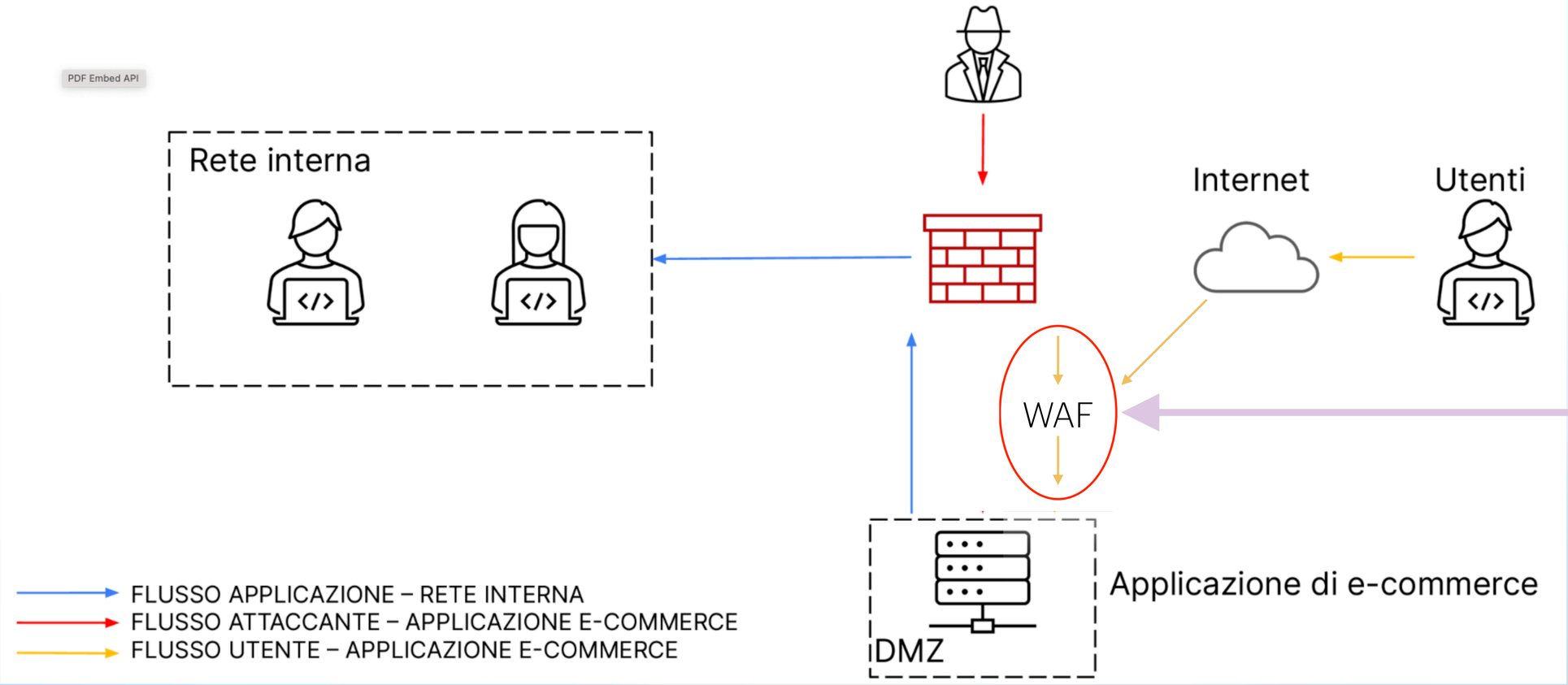
Come prima Task, ci viene chiesto quali potrebbero essere le azioni preventive che noi possiamo adottare per implementare la difesa della nostra applicazione Web, da attacchi di tipo SQLi oppure Xss, da parte di un attaccante. Andiamo a riprendere brevemente la tipologia ti attacchi:

- SQLi: Permette ad utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un applicazione web.

- XSS: Ovvero una famiglia di vulnerabilità che permettono ad un potenziale attaccante di prendere il controllo su una Web App e sulle sue componenti con un impatto devastante sulla sicurezza degli utenti.

Task 1: Azioni preventive

Azioni preventive



Aggiungiamo un WAF a protezione della nostra DMZ.

Task 1: Azioni preventive

Introduzione di un WAF

Tra le azioni preventive di maggior impatto, come visto nella slide precedente, ho aggiunto un WAF, ovvero un Web Application Firewall. Esso è uno strumento di sicurezza informatica progettato per proteggere le applicazioni web da minacce e attacchi online. Funziona filtrando il traffico HTTP e monitorando il traffico tra un'applicazione web e l'utente finale. Il WAF analizza le richieste web in ingresso e in uscita, identificando, (tramite uno spacchettamento dei pacchetti) e bloccando attacchi comuni come SQL injection, cross-site scripting (XSS), tentativi di accesso non autorizzati e altri tipi di vulnerabilità web. In questo modo proteggiamo anche la rete interna. Ovviamente oltre all'implementazione del WAF, dobbiamo assicuraci di mantenere le nostre Web app aggiornate con le ultime patch di sicurezza disponibili, ed eseguire con regolarità dei Penetration testing, per identificare e correggere, se presenti, le vulnerabilità prima che vengano sfruttate.

Task 2: Impatti sul business

Supponendo che l'azienda subisca un attacco ddos, che rende l'applicazione non raggiungibile per 10 minuti, calcoliamo l'impatto che questo attacco ha, a livello economico.

Si suppone che l'azienda, ogni minuto guadagni 1500€, da acquisti degli utenti, che non potendo acquistare per 10 minuti, l'azienda subirà un danno ipotetico pari a 15000€.

Questo ci fa capire che gli attacchi talvolta non vertono sul furto di informazioni, ma semplicemente vogliono creare un disagio all'azienda, rallentando l'accesso alla piattaforma di acquisto e rendendola inaccessibile.

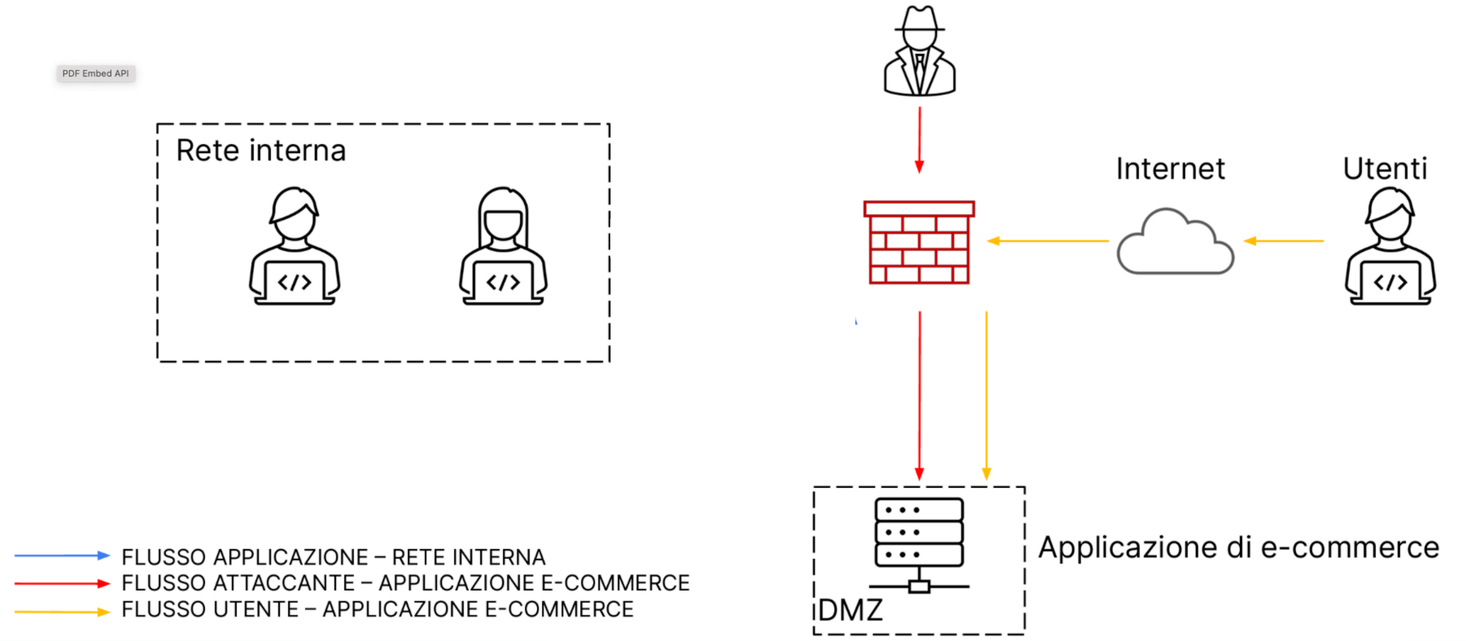
Prendendo spunto da questo attacco vorrei introdurre, un accenno al DRaas, ovvero il tentativo di mantenere operativo il servizio attraverso un modello di cloud chiamato Disaster Recovery As A Service, dove il provider mette a disposizione un'infrastruttura in cloud che viene immediatamente attivata in caso di disastro sul sito primario della compagnia, che sia un disastro naturale, o un attacco di questa portata.

Sicuramente è svantaggioso in termine di tempistiche, a causa dello switch tra un sito primario ad uno secondario, tuttavia però in termini di ottimizzazione del budget, è spesso la soluzione migliore considerato che si pagherebbe il servizio solo in caso di effettivo utilizzo. Quindi mettendo il caso che l'attacco duri più di 10 minuti, possiamo far si che il nostro servizio continui, ammortizzando il costo del disagio causatoci, e mantenendo il servizio attivo.

Task 3: Limitare i danni

Se l’applicazione web viene infettata da un malware, ormai dobbiamo cercare di limitare i danni evitando che si propaghi sulla rete interna. I malware sono software dannosi progettati per danneggiare, interrompere, rubare informazioni o ottenere l'accesso non autorizzato a sistemi informatici o dispositivi. La difesa dai malware coinvolge l'uso di software antivirus, firewall, aggiornamenti regolari del sistema e delle applicazioni, così come l'educazione degli utenti per evitare comportamenti rischiosi come il clic su link sospetti o il download da fonti non attendibili. Ma nulla è veramente al sicuro, se è accessibile. L’unico modo per avere un rate del 100% della sicurezza è isolarlo dal mondo esterno, e come sappiamo, la sicurezza fa a pugni con l’accessibilità, per questo occorre adottare misure preventive, e tenere l’asticella dell’attenzione sempre in alto.

Task 3: Incident Response



In questo caso parliamo di isolamento, che consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora di più l'accesso alla rete interna da parte dell'attaccante, che potrà continuare ad avere accesso all'area contaminata.

Task 3

Cos'è successo?

Nella Task 3, è accaduto un incidente di sicurezza, ovvero una violazione ad un sistema informatico, o la minaccia imminente di una violazione. Esempi posso essere perdita o fuoriuscita di informazioni sensibili o private, un'intrusione nei sistemi interni della compagnia da parte di un hacker, o come nel nostro caso un attacco malware.

Esiste un team che si occupa di queste casistiche, ovvero il CSIRTs (Computer Security incident response teams). In presenza di un incidente di sicurezza, essi devono essere in grado di rispondere all'incidente di sicurezza in maniera calma e consistente. La situazione di crisi, se non correttamente gestita, può portare a decisioni errate tali da compromettere il business di una compagnia.

Analizziamo insieme la fase di rilevamento e analisi del team. Iniziamo con il mettere in atto le prime attività per scoprire come è avvenuto l'incidente, quali sistemi ha impattato e quali potrebbero essere i prossimi sistemi a rischio. Una volta completate la valutazioni, il team deve trovare una soluzione per ridurre a stretto giro gli impatti dell'incidente. Inizia formalmente la fase di contenimento, che era quella richiesta dalla traccia per poi passare alla fase di eliminazione e recupero.

Una volta contenuta la minaccia, e aver conclusa la fase precedente, si fa un analisi, post- incidente, che ci è di enorme aiuto, perché ci permette di imparare dai nostri errori, facendoci analizzare le motivazioni dietro la breccia al nostro sistema. Utilizzando le informazioni acquisite potremo non solo migliorarci ma rendere la nostra fase di preparazione molto più prestante nel futuro.

Fin.