REPORT CASO REALE : ANALISI LOG

Prendiamo in esame tre ipotetici casi reali di attacchi malevoli a contesti aziendali, esaminandone le dinamiche e le possibili soluzioni risolutive.

Trattasi quindi di incidenti di sicurezza, o eventi, ossia qualsiasi violazione informatica o fisica che minacci la confidenzialità, integrità o disponibilità (CIA) dei sistemi, processi o dati sensibili di un'organizzazione.

Necessario ai fini della presa d'azione del team predisposto all'Incident response è la definizione di criticità dell'incidente (Scala degli impatti) in base a criteri come : Impatto su quantità e tipologia di servizi critici coinvolti dall'incidente, impatto d'immagine, impatto economico provocato sugli asset aziendali e perdite economiche in caso di pesanti disservizi.

IMPATTO SU BUSINESS

Sulla base di queste classificazioni, ne verranno applicate altre per dettagliare esattamente il tipo di perdita funzionale ed economico stimata dalla compagnia in caso di avvenuto incidente.

CRITICITÀ	IMPATTO SUI SERVIZI (FUNZIONALE)	IMPATTO FINANZIARIO
NESSUNA	Nessun impatto sui servizi e sugli utenti. La compagnia riesce a fornisce tutti i servizi a tutti gli utenti	La compagnia non si aspetta nessuna perdita economica
BASSA	Minimo impatti su servizi ed utenti. Tutti i servizi critici erogati dalla compagnia sono attivi	La compagnia si aspetta un impatto economico limitato (e.g. 10.000€)
MEDIA	La compagnia non riesce ad erogare alcuni dei servizi critici o parte di essi ad un sottoinsieme limitato di utenti	La compagnia si aspetta un impatto economico non indifferente (e.g. 10.000 / 500.000€)
ALTA	La compagnia non riesce ad erogare servizi critici per tutti gli utenti	La compagnia si aspetta un grosso impatto economico (e.g. >500.000€)

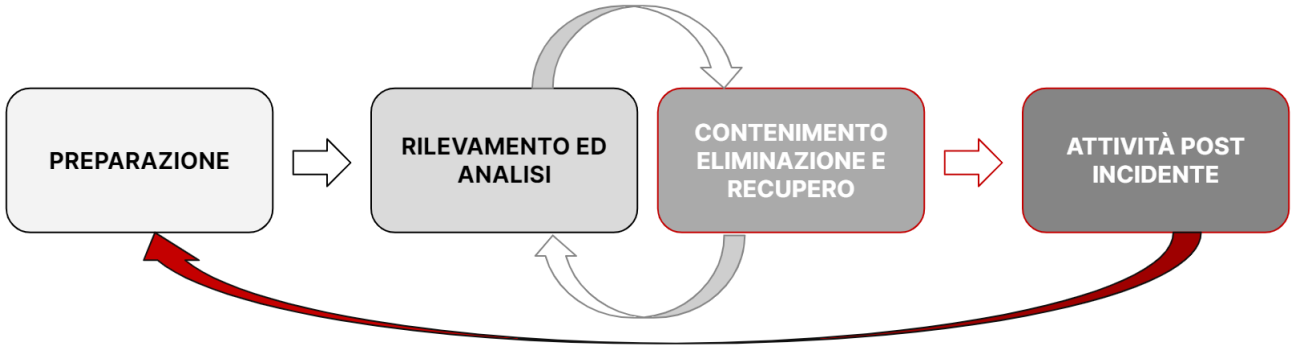
Fatte queste doverose premesse, analizziamo il caso proposto di ipotesi su impatto business.

Nel caso in cui un applicazione web subisse un attacco di tipo Ddos (Distribuited Denial of Service) che mira ad interrompere le attività aziendali tramite uso massivo di richieste fino alla completa saturazione, rendendolo di fatto non più disponibile per l'utenza.

Ipotizzando quindi che un'applicazione rimanga irraggiungibile per dieci minuti, e che i guadagni al minuto ammontino a 1.500 $, la perdita prevista sul business sarà di 15.000 $, un impatto finanziario di criticità classificata come MEDIA.

AZIONI PREVENTIVE SQL/XSS ATTACKS

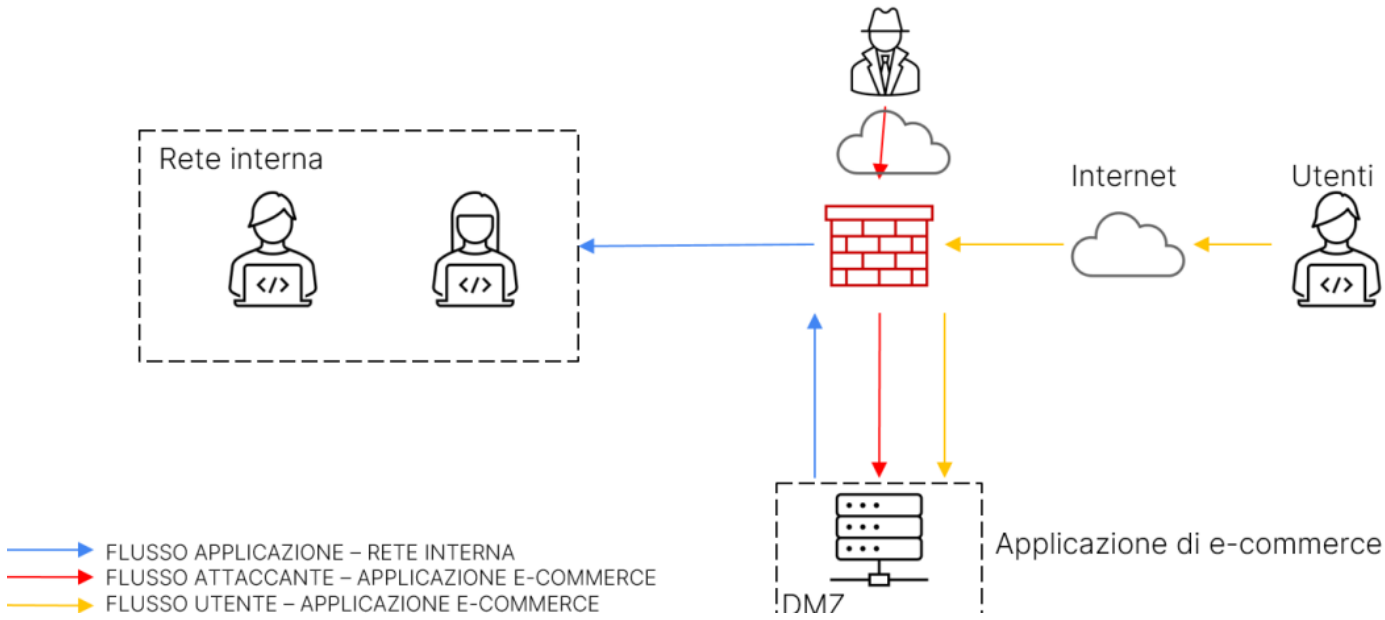
Coloro che sono addetti alla risposta pronta ed efficace agli incidenti di sicurezza aziendali sono i componenti del team CSIRT(Computer Security Incident Response Team) che hanno il compito di intercettare, analizzare e rispondere alla minaccia tramite policy e procedure di incident response preventivamente pianificate in fase di preparazione . Il CSIRT risponde alle minacce tramite un processo diviso in fasi.



La prima contromisura da attuare però, ancor prima della “response” è sicuramente la prevenzione, ossia l’adottare tutte le misure di sicurezza possibili affinchè si riduca sensibilmente il rischio che l’incidente si verifichi.

Con questa premessa, analizziamo il caso ipotetico in cui si vede necessaria la protezione di un’applicazione web da attacchi di tipo SQL injection (Structured Query Language) e XSS (Cross Site Scripting), attacchi che si basano sull’iniezione di codice malevolo tramite vulnerabilità al fine di raccogliere, manipolare e reindirizzare informazioni riservate.

La struttura di rete compromessa dataci in esame è la seguente:

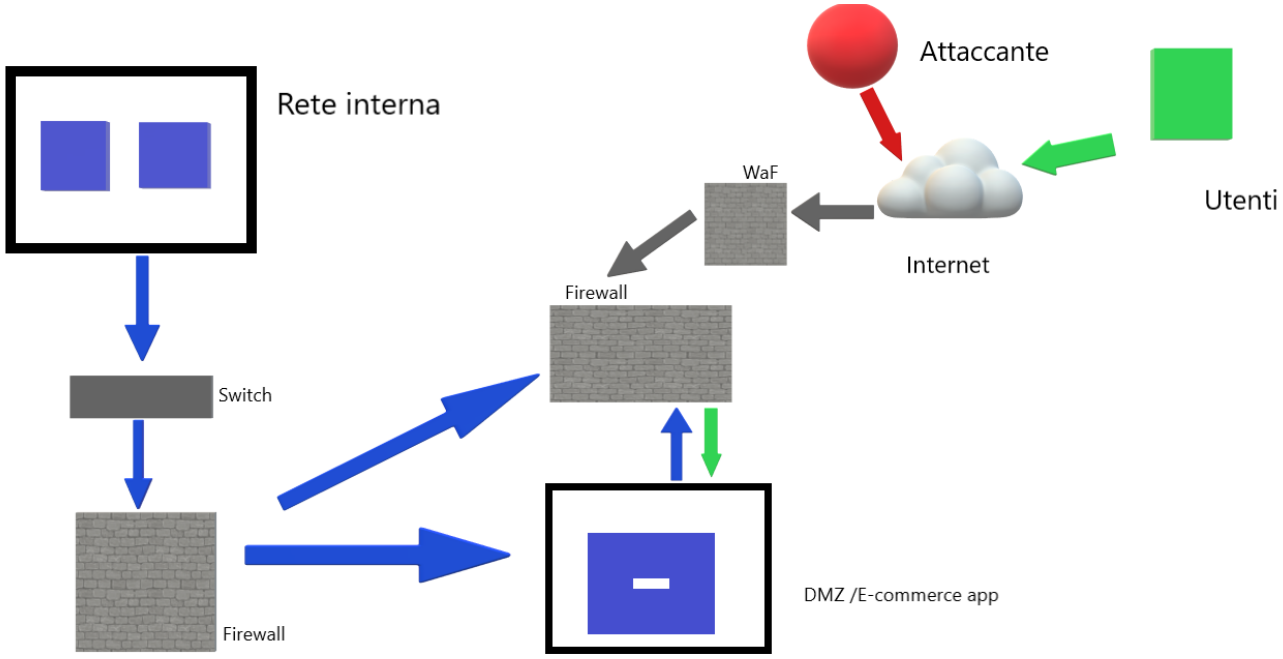


In cui l’utente malevolo supera il Firewall attaccando l’applicazione in DMZ (DeliMilitarized Zone) e conseguentemente avendo accesso anche a rete interna.

La DMZ dovrebbe aggiungere un ulteriore livello di sicurezza ad una rete aziendale, facendosi sì che un nodo esterno possa accedere soltanto ai servizi e non alla rete interna.

Per eliminare la possibilità di un qualsiasi tipo di Code injection, risulta necessaria l’aggiunta di un WAF (Web Application Firewall) proteggendo appunto l’applicazione web da attacchi, traffico internet indesiderato come bot, Dos e injection.

Potremmo quindi considerare una struttura di rete che si presenti cosi:



Come si può notare è stato aggiunto un WAF, una versione specializzata di un firewall per controllare gli accessi alle risorse di sistema con sistema di filtraggio traffico aggiungendo pro attività e intelligence.

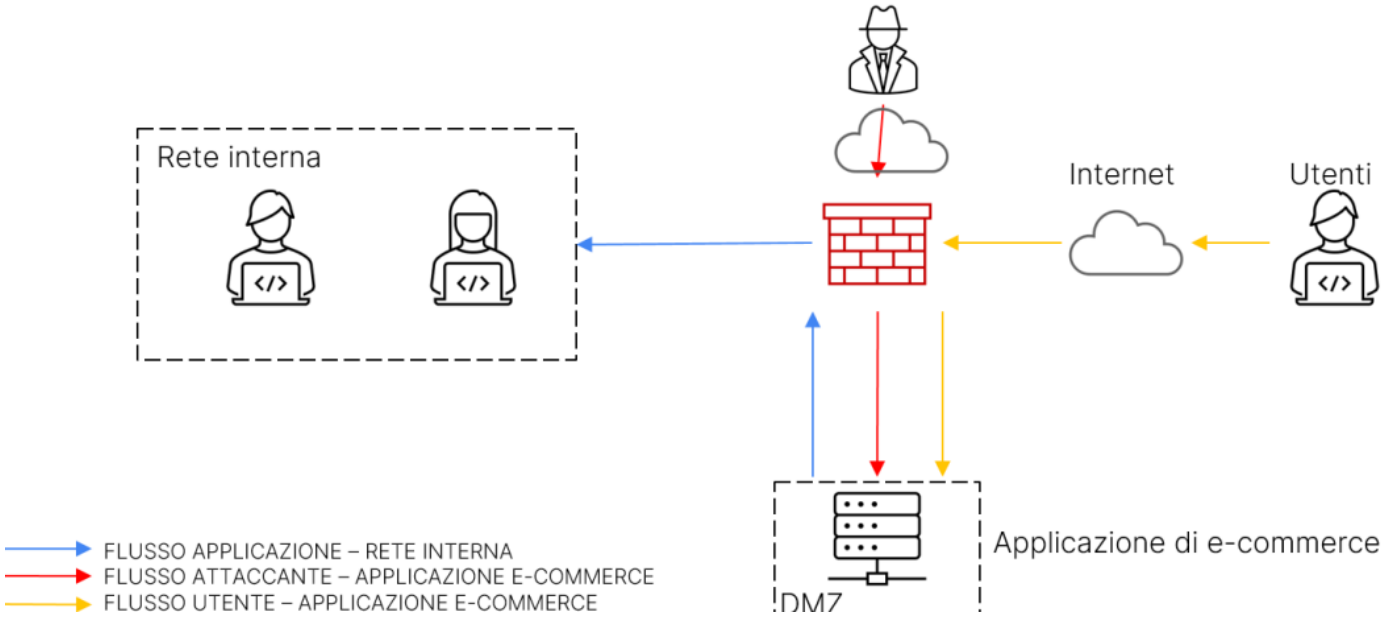
Inoltre, per ulteriore sicurezza l'implementazione di un firewall ssl inspection, e l'introduzione di uno switch per l'indirizzamento di pacchetti unicast solo a porte associate ad indirizzo di destinazione, risolvendo anche il problema di identificazione delle periferiche.

Si consiglia altresì una buona sanificazione di corretto input, utilizzare solo procedure memorizzate per richieste database , e un monitoraggio attivo degli eventi ed analisi anomalie, e sistemi di IPS (Intrusion Prevention System) componenti software che individuano e registrano info relative, segnalando e bloccando le attività dannose.

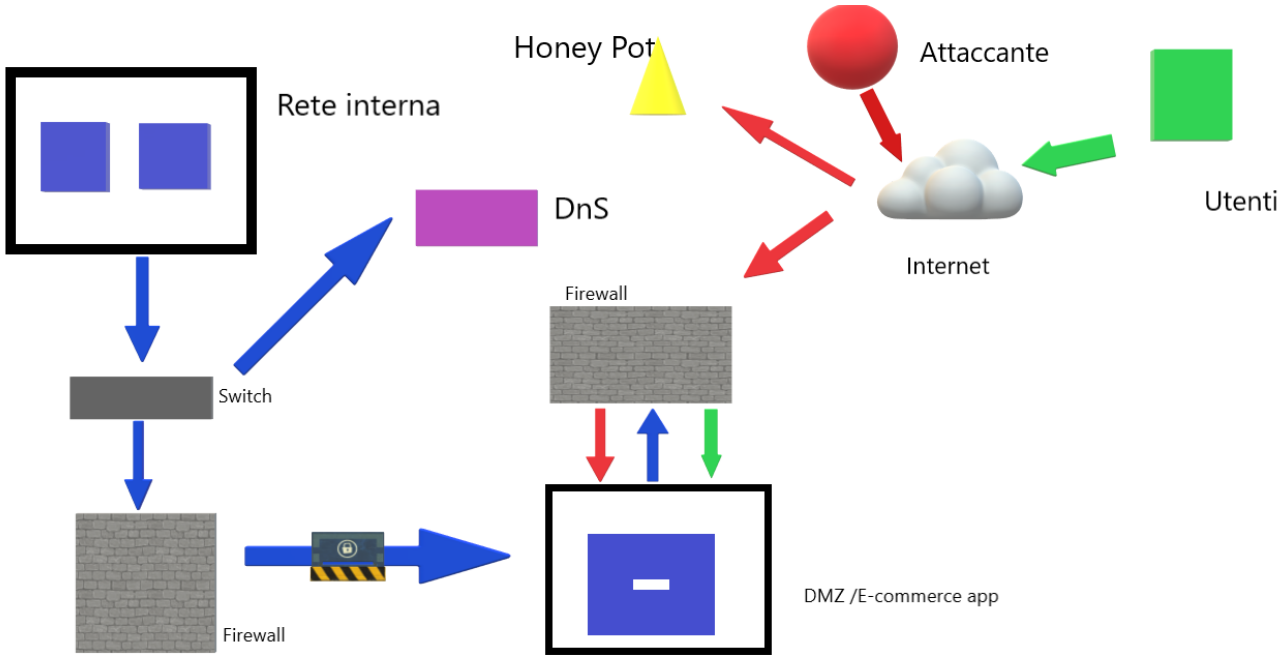
RESPONSE

Prendiamo adesso in esame uno scenario ipotetico in cui in una fase di monitoraggio ci si accorga che un'applicazione web sia stata infettata da un malware, la priorità di risposta viene in questo caso consistono nel contenimento della minaccia, non rimuovendo l'accesso dell'attaccante alla macchina infetta.

La situazione iniziale di rete è sempre la seguente:



Si potrebbe ipotizzare una rete impostata come segue :



La struttura è molto simile a quella precedente, intendendo mantenere l’accesso dell’attaccante alla macchina infetta si dovrebbe quindi procedere ad una segmentazione di rete, limitando la riproduzione e l’accesso al resto della rete non rimuovendone però totalmente l’accesso mediante VLAN , domini che permettono di

segmentare la rete a livello logico quindi per funzione o applicazione, e non fisico, dando la possibilità di bloccare le comunicazioni tra VLan diverse (Tramite router).

Implementazione di switch per supporto di rete in layer, abilitazione filtri MAC e funzionalità di controllo accessi.

Sarà opportuno creare una nuova DMZ non compromessa che funga da barriera tra una zona aziendale e l'altra, Introdurre sistemi di IPS/IDS per protezione e rilevamento intrusioni.

L'introduzione di misure di protezione contro DNS tunneling , usando estensioni DNS specifiche (DNSSEC) che autenticano le risposte, evitando che si venga reindirizzati in siti web errati/contaminati.

Come misura preventiva, potrebbe inoltre essere necessaria l'introduzione di un Honeypot trap, un finto punto d'ingresso volutamente vulnerabile ed attentamente monitorata, in questo modo si potrebbe contenere un numero non indiferrente di attacchi, recuperando tempo prezioso di response "incastrando" l'attaccante nell'honeypot ed analizzandone i movimenti per individuare future intromissioni simili o uguali.