Oggi andremo ad analizzare una rete aziendale che offre un servizio di e-commerce. Nell'area dmz è ovviamente presente il server che offre il servizio e-commerce che a sua volta, grazie ad una policy "allow" del firewall che fa da intermediario con la rete interna, puo raggiungere quest'ultima. Se un black hater dovesse riuscire ad attaccare il server e-commerce, di conseguenza potrebbe raggiungere la rete interna e creare danni gravi.

PUNTO 1

La prima richiesta dell'azienda è quella di proteggere il server web da eventuali attacchi sql ed xxs.

Come membro del SOC designato per le security operation da attuare per questa particolare azienda, mi sono preso la libertà di attuare modifiche alla rete aziendale perchè osservandola ha diverse lacune.

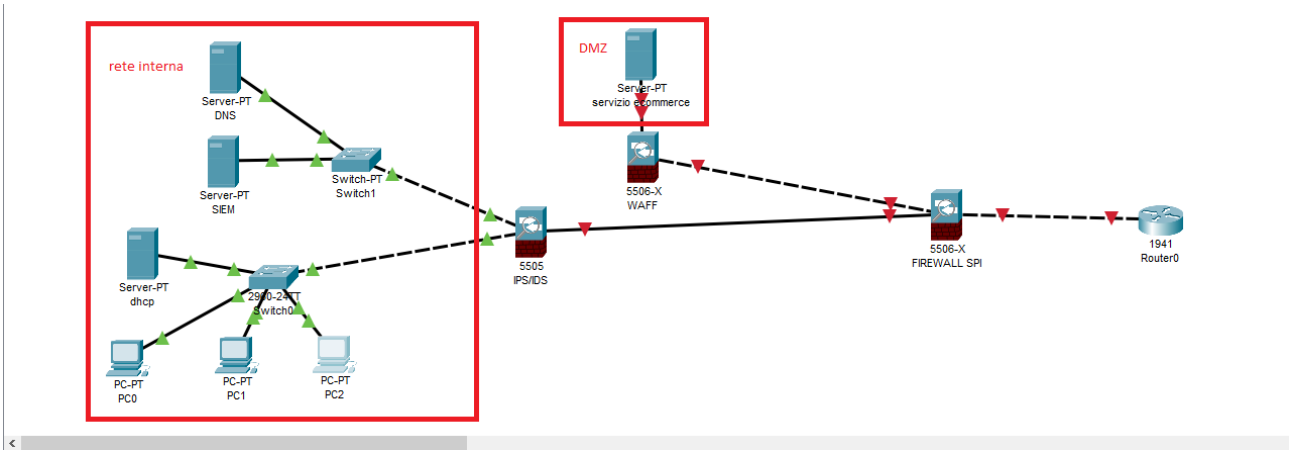
Le soluzioni io adotterei sono le seguenti:

1)Innanzitutto introdurrei, frapposto fra l'area dmz ed il firewall un'ulteriore firewall ma piu specifico: il WAF, che nello specifico difende il web server da attacchi xss ed sql che, come sappiamo, sono fra i piu potenti che si possono effettuare contro web app. Con questa semplice aggiunta, risolvo la questione richiesta nel punto 1 dall'azienda.

2)In più metterei due ulteriori firewall specifici, l'IDS e l'IPS che, rispettivamente, rilevano le intrusioni e prevengono le intrusioni riferendole all'amministratore di sicurezza.

3)Un 'ulteriore implemento che farei e quello di mettere un firewall SPI, che oltre al controllo, traccia e da informazioni su tutte le connessioni passate attraverso il firewall in modo che, se dovessimo notare una connessione sospetta, potremmo intervenire tempestivamente.

4)Cosa piu importante di tutte, Utilizzerei il SIEM, un software che permette di raccogliere centralmente i log da diverse sorgenti, quali firewall, router ecc. Lo installerei su un server, come accennato, centralizzato, in modo tale da vedere in real time informazioni fondamentali quali i log che, se sospetti, potrebbero antecedere un attacco e quindi ci darebbero il tempo di intervenire.



Come possiamo vedere, la rete interna è protetta da un firewall ips/ids che previene intrusioni ed all'interno della sala server interna, ho messo un server su cui ho installato il software SIEM per analizzare in tempo reale i log delle diverse sorgenti aziendali. Nell'area DMZ,quindi raggiungibile dalla rete esterna (internet) in cui c'è il server e commerce, ho messo un firewall WAFF che previene e difende il server da eventuali attacchi SQL o XSS ed infine ho specificato il firewall in entrata dopo il router, adottando un

firewall SPI che, essendo piu avanzato di un firewall normale, mi traccia informazioni preziose sulle connessioni in entrata.

PUNTO 2

Dopo che il security operation center (SOC) imposta la rete nella maniera piu sicura possibile, si presenterà comunque la casistica in cui un attacco abbia effetto. Nello specifico ipotizziamo che l'azienda subisca un attacco DOS che rende il sito, che frutta 1500 euro al min,inagibile per 10 min.

Per prima cosa creerei un BIA (business impact analysis) per capire quanto l'attacco ha impattato sull'azienda.

A prima occhiata, intuendo il servizio, si evince che il parametro qualitativo da assegnare in seguito all'attacco effettuato è abbastanza alto, in quanto un sito che offre servizi di e-commerce deve dimostrare solidità al cliente che compra con una carta di credito e, se vulnerabile ad attacchi, viene meno questa sicurezza. Anche il parametro quantitativo e alto, in quanto in soli 10 minuti l'azienda riesce a fatturare grazie al sito 15000 euro. Altri parametri che darei all'incidente avvenuto, è quanto tempo il servizio puo in effetti non funzionare (MTD), senza che le conseguenze siano catastrofiche, ed il tempo che si impiegherà per neutralizzare l'attacco e il risolleva mento del server (RTO), facendo in modo che l'MTD non sia mai maggiore del RTO. Una volta analizzato l'incidente ed averlo classificato secondo l'impatto che ha avuto sull'azienda, studierei una strategia per far si che non riaccada.

Le soluzioni che adotterei sono l'abolizione dello SPOOF (single point failure) implementando il Failover cluster, ovvero l'aggiunta alla rete aziendale di un secondo server, identico al primo, che svolga lo stesso ruolo e possa essere usato in casi come questi.

Un'altra soluzione che implementerei è, tenendo conto della possibilita economica dell'azienda, di, come si dice in gergo tecnico, "migrare verso il cloud", ovvero demandare il compito di DR a grandi colossi come google o amazon e,se la soluzione risultasse troppo dispendiosa, di adottare una soluzione Draas, molto simile all'ultima citata, differente solo nel fatto che la soluzione dell'uso di un modello cloud viene effettuta solamente ad incidente avvenuto.

PUNTO 3 e 4

In questa casistica, ci ritroviamo a dover affrontare un malware che è stato iniettato nell'applicazione web ed ovviamente non dobbiamo lasciare che il malware raggiunga la rete interna, dando modo magari all'attaccante di rubare dati sensibili e fare danni ancora piu grandi.

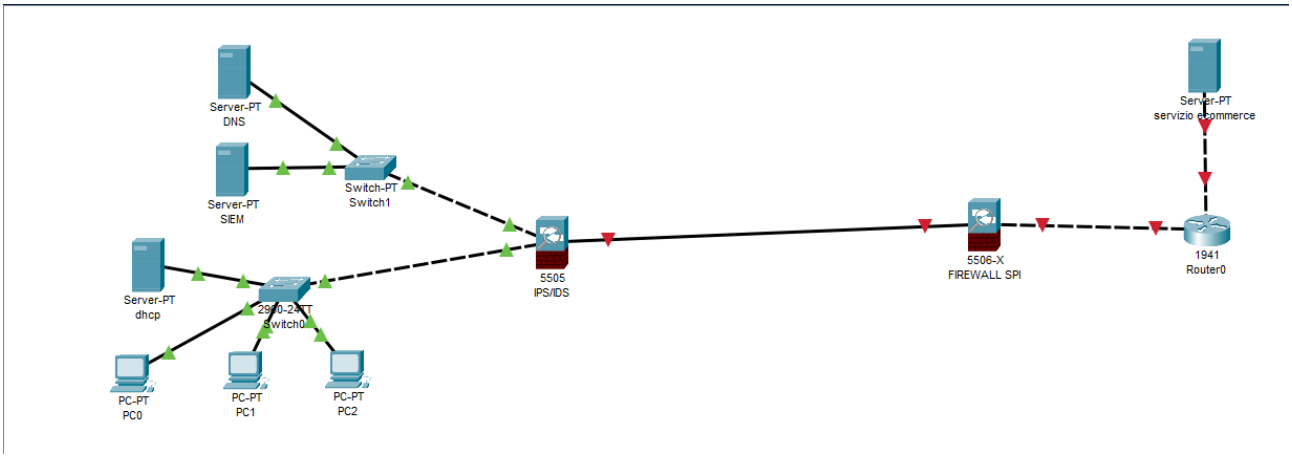
In questo caso, come membro del CSIRTs, devo fare in modo che ciò non avvenga.

Le misure che adotterei:

Innanzitutto classificherei l'incidente come "incidente web",essendo eseguito tramite sito web.

Poi analizzerei i log e le informazioni utili (alert) catturate dal firewall, l'antivirus ecc. (o, meglio ancora, dal SIEM se l'azienda deciderà di attuare questa modifica alla rete). Una volta che mi sono fatto il quadro della situazione ed aver assegnato un livello di criticità all'incidente (in questo caso ho assegnato criticità media, dato che si tratta di un sito e-commerce e se si riuscisse ad arrivare alla rete interna l'impatto sarebbe grande), devo intraprendere la fase di contenimento , rimozione e riduzione dell'incidente, che è la più importante.

In primis, isolerei il server infetto non rimuovendolo (in questo caso si può comunque analizzare il modo in cui è riuscito e stato eseguito l'attacco):



Come possiamo vedere, il server infetto al momento e completamente fuori dalla rete aziendale. Non è stato ne spento ne staccato, quindi è ancora "funzionante" e "manovrabile" dal black hater in questione, però non ha accesso alla rete aziendale se non tramite internet.

Un'altra implementazione che attuerei è la seguente:

Partendo dal presupposto che esista un database del sito con dati dei clienti e sulle transazioni, è importante non perderli e far si che non siano compromessi. Infatti configurerei un RAID 5, ovvero 3 dischi che cooperano fra di loro ed, in caso di attacco o malfunzionamento, possono sostituirsi copiando i dati dal disco rotto/infetto, per poi decidere quale azione fare (se purge,destroy o clear) cercando di capire quanto sia compromesso e tenendo anche conto della disponibilità economica dell'azienda (ad esempio se si decidesse di distruggerlo(destroy) bisognerebbe comprarne uno nuovo).

Una volta svolte tutte le analisi sul server in questione ed aver capito da dove l'attaccante è entrato e quale vulnerabilità ha sfruttato, bisogna capire se il server in questione è ancora utilizzabile e non compromesso. Infine, traggo le mie conclusioni e studio ciò che poteva esser stato fatto meglio o meno per far si che, in un eventuale futuro, se si dovesse ripresentare l'incidente poco sopra menzionato, le remediation attuate possano essere ancora perfezionate.