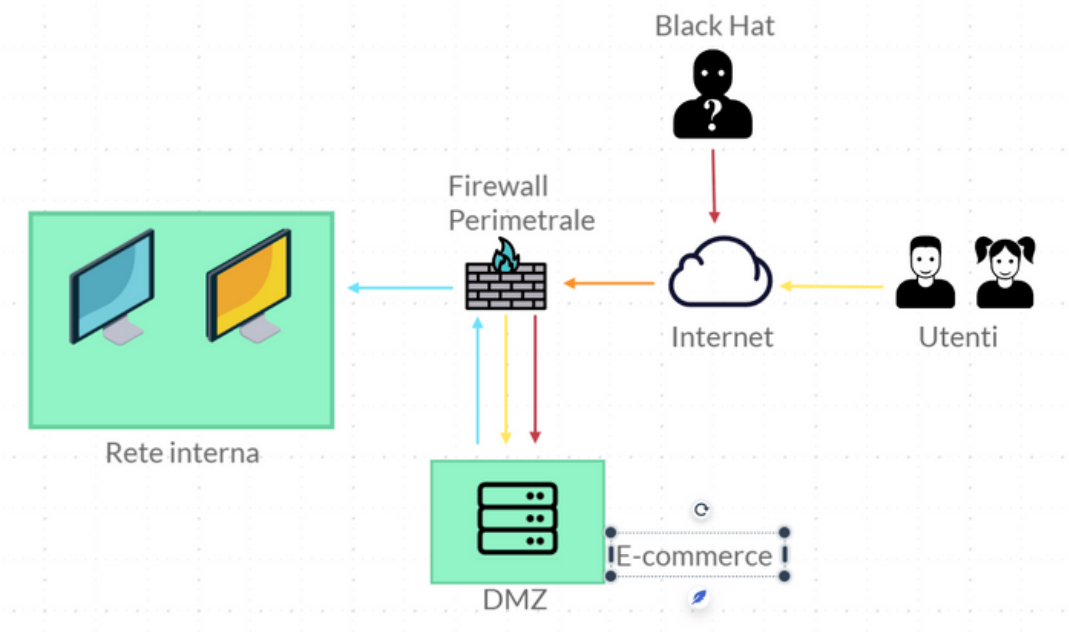
S9L5

1 - AZIONI PREVENTIVE
2 - IMPATTI SUL BUSINESS
3 - RESPONSE

Traccia



1-Modificare l'immagine in figura in modo da evidenziare le implementazioni per prevenire attacchi SQL e XSS da parte di utenti malintenzionati al servizio WEB di e-commerce.

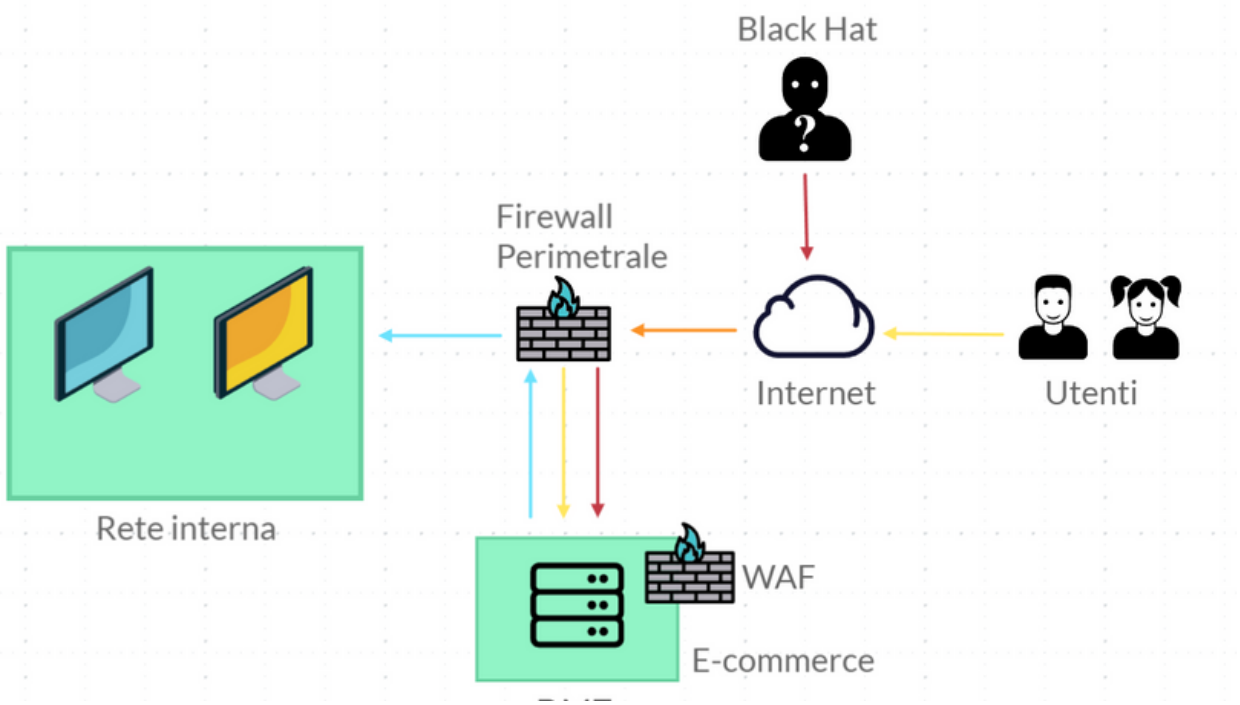
2-Presumendo che l'applicazione Web subisca un attacco di tipo Ddos rendendola non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto a questa conseguenza, considerando che ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

3-Modificare l'immagine in figura presumendo che il servizio WEB sia stato infettato da un Malware e la vostra priorità è quella di non far si che si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

S9L5

1 - AZIONI PREVENTIVE ✓
2 - IMPATTI SUL BUSINESS
3 - RESPONSE

Azioni preventive



Per prevenire gli attacchi da utenti malintenzionati al nostro servizio WEB di e-commerce è necessario ampliare il nostro sistema di rete aggiungendo un WAF "Web Application Firewall". Il WAF funge da scudo difensivo, rilevando e bloccando attacchi comuni come SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) e altri exploit che mirano alle vulnerabilità delle applicazioni web.
Questi attacchi possono compromettere la sicurezza dei dati e danneggiare l'integrità delle applicazioni web ed i suoi utenti esaminando il traffico in ingresso e in uscita dalla nostra applicazioni web, filtrando eventuali contenuti malevoli o comportamenti sospetti.

S9L5

1 - AZIONI PREVENTIVE ✓
2 - IMPATTI SUL BUSINESS ✓
3 - RESPONSE

Impatti sul business

Calcolo dell'impatto finanziario:

1. Valore Medio dell'Utente al Minuto:
   - Si assume che ogni minuto gli utenti spendano in media 1.500 € sulla piattaforma.
2. Durata dell'Interruzione:
   - L'attacco DDoS causa un'interruzione di 10 minuti.
3. Calcolo dell'Impatto Finanziario:
   - Impatto Finanziario = (Valore Medio al Minuto) x (Durata dell'Interruzione)
   - Impatto Finanziario = 1.500 €/minuto x 10 minuti

L'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.

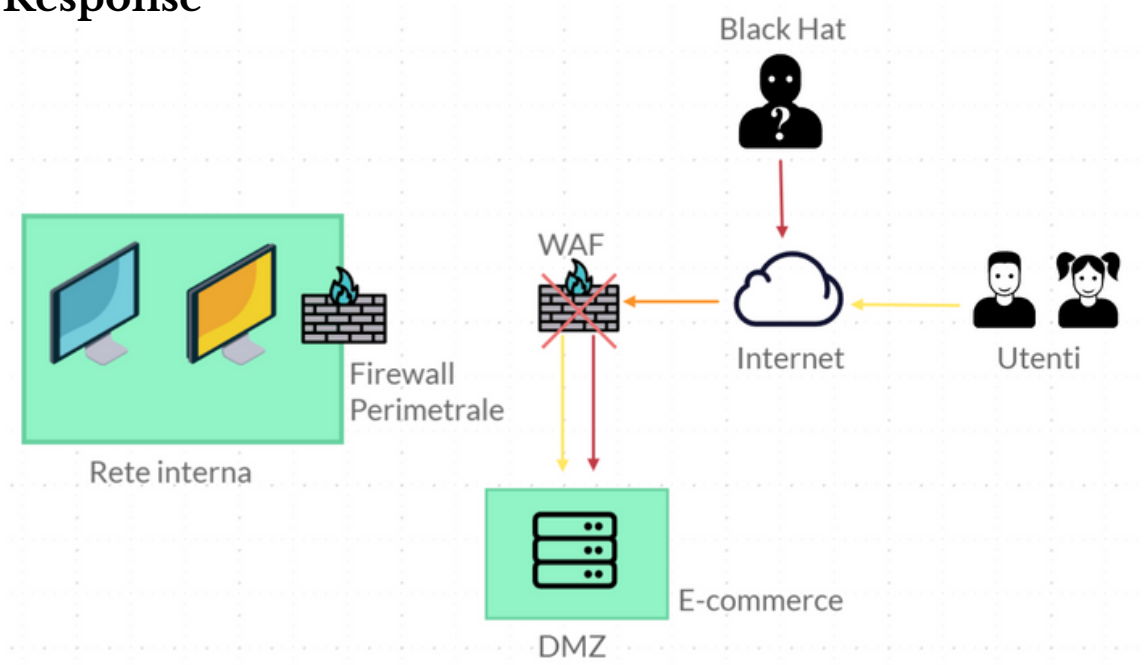
Il processo che coinvolge l'identificazione, la valutazione e la gestione dei rischi in ambito della sicurezza informatica si basa su questa pratica e serve per comprendere e mitigare tali minacce dei sistemi informatici.

1. Identificazione delle Minacce:
   - La valutazione dei rischi inizia con l'identificazione delle minacce alla sicurezza informatica. L'obiettivo è riconoscere e comprendere le potenziali minacce che possono mettere a rischio la nostra sicurezza
2. Valutazione dell'Impatto Finanziario:
   - Questa fase mira a quantificare le possibili perdite finanziarie che potrebbero derivare da un particolare scenario di minaccia
3. Valutazione della Probabilità:
   - Oltre all'impatto finanziario, la valutazione del rischio coinvolge la stima della probabilità che l'attacco si verifichi.
4. Identificazione di Contromisure:
   - Sulla base dell'analisi del rischio, vengono identificate le contromisure da adottare per mitigare l'impatto delle minacce.
5. Pianificazione e Miglioramento Continuo:
   - La gestione della sicurezza informatica prevede una pianificazione strategica per affrontare e prevenire le minacce in corso e future.

S9L5

Response

1 - AZIONI PREVENTIVE ✓
2 - IMPATTI SUL BUSINESS ✓
3 - RESPONSE ✓



Come in figura si può notare il Black Hat è riuscito a superare il nostro WAF ed ha infettato il servizio WEB con un malware, di conseguenza dobbiamo fare in modo di isolare il dispositivo infetto dalla nostra rete interna evitando ulteriori danni.
Detto ciò abbiamo eliminato tutte le connessioni tra il servizio WEB e la nostra rete interna assicurandoci la protezione della nostra infrastruttura creando una situazione di Air gap.
L'isolamento di un sistema infetto è una tecnica di sicurezza informatica che serve a limitare la propagazione di un'eventuale infezione da malware o minaccia informatica all'interno di una rete.
L'obiettivo principale dell'isolamento in questo caso è contenere il rischio di diffusione del malware sulla nostra infrastruttura ma continuando a garantire l'accesso agli utenti (Pratica non conforme alla tutela degli Utenti in quanto potrebbero essere infettati anche loro).
Ecco una diversa tecnica utile per mitigare tali minacce sul servizio WEB.
Sandboxing avanzato:
Il sandboxing è implementato durante la progettazione e lo sviluppo dei software per prevenire tali minacce, utilizzando le tecniche di sandboxing consentiamo l'esecuzione del servizio WEB infetto in un ambiente controllato e senza interrompere l'accesso degli utenti. Questa pratica è una strategia efficace per mitigare i rischi e ridurre l'impatto di un'eventuale compromissione però non può garantire un isolamento del sistema al 100%.