Progetto S9_L5

22/03/2024

Cyber Security &
Ethical Hacking

Manuel Buonanno

Indice

Traccia

Con riferimento alla figura in slide 3, 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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

5. Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).

-

-

Bonus

Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

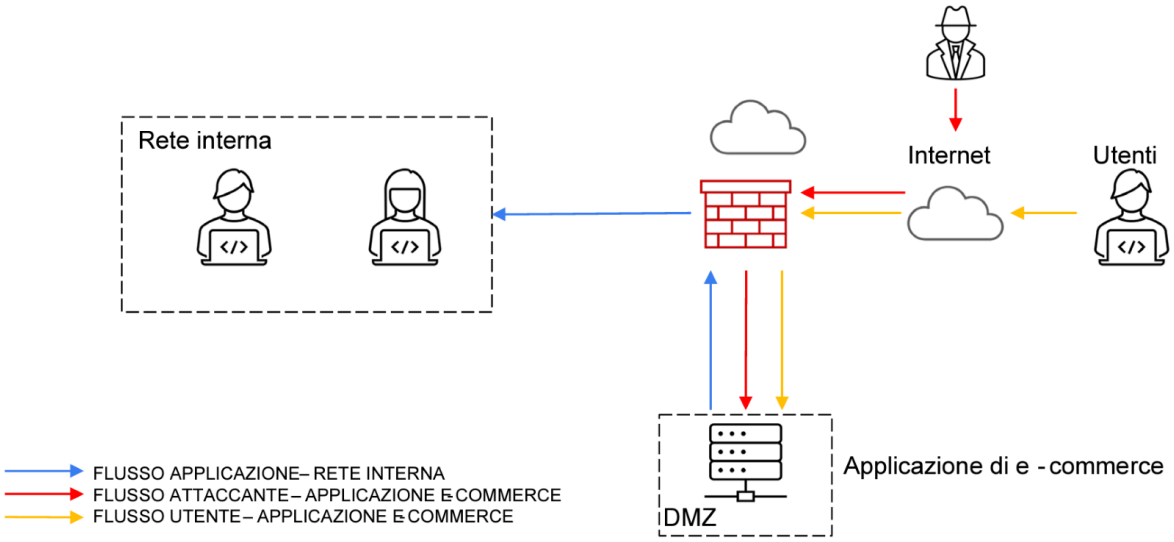
https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

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 DMZ venisse compromesso, potenzialmente un attaccante potrebbe raggiungere la rete interna.



Brevi nozioni teoriche prima dello svolgimento

Firewall
Un firewall è un dispositivo o un software progettato per controllare e filtrare il traffico di rete in entrata e in uscita. Può essere utilizzato per proteggere una rete informatica impedendo a traffico non autorizzato o dannoso di raggiungere i dispositivi all'interno della rete. Utilizzeremo in questo caso un Web Application Firewall (WAF): Un WAF è un tipo di firewall a livello di applicazione progettato per proteggere le applicazioni Web da minacce come SQL injection (SQLi), cross-site scripting (XSS) e altri attacchi comuni.

Rete Interna
La rete interna è la parte di una rete informatica che si trova all'interno delle strutture dell'organizzazione e non è direttamente esposta a Internet.

DMZ (Demilitarized Zone)
Una DMZ è una zona di rete separata e protetta che si trova tra la rete interna e Internet. Viene utilizzata per ospitare servizi e applicazioni accessibili dall'esterno, come server Web pubblici.

SQL Injection (SQLi)
Un attacco SQL injection consiste nell'inserire codice SQL dannoso in input di un'applicazione Web per manipolare le query del database e ottenere informazioni non autorizzate o compromettere la sicurezza del sistema.

Cross-Site Scripting (XSS)
Un attacco XSS consiste nell'iniettare codice JavaScript malevolo in pagine Web visualizzate da altri utenti. Può essere utilizzato per rubare cookie di sessione, informazioni sensibili o eseguire azioni non autorizzate.

DDoS (Distributed Denial of Service)
Un attacco DDoS è un tentativo deliberato di sovraccaricare un servizio online, come un sito Web o un'applicazione, generando un volume massiccio di traffico da diverse fonti.

Malware
Il malware è un software dannoso progettato per infiltrarsi, danneggiare o compromettere un sistema informatico senza il consenso dell'utente. Include virus, worm, trojan, ransomware, spyware, etc.

Azione preventiva per un attacco
Un'azione preventiva per un attacco è una misura o una strategia proattiva adottata per proteggere un sistema o una rete da minacce informatiche. Include l'implementazione di controlli di sicurezza, la formazione degli utenti, la gestione delle patch, ecc.

SIEM (Security Information and Event Management)
SIEM è una piattaforma che raccoglie, analizza e interpreta i log di sicurezza e gli eventi da diverse fonti per fornire una visibilità completa sulla sicurezza della rete e facilitare la risposta agli incidenti di sicurezza.

SOAR (Security Orchestration, Automation, and Response)
SOAR è una piattaforma che automatizza la risposta agli eventi di sicurezza, coordinando le azioni tra diversi strumenti di sicurezza e accelerando la risposta agli incidenti.

Disaster Recovery
Disaster Recovery è il processo di ripristino di un sistema o di una rete informatica a seguito di un disastro o di un evento catastrofico, come un attacco informatico, un guasto hardware o un'interruzione di servizio.

Business Continuity Plan
Il Business Continuity Plan (BCP) è una strategia proattiva per garantire la continuità delle operazioni aziendali in caso di interruzione o disastro. Include la pianificazione delle risposte agli incidenti, il ripristino dei servizi e la gestione delle crisi.

Azioni preventive

Per difendere un'applicazione Web da attacchi di tipo SQL injection (SQLi) o cross-site scripting (XSS) da parte di utenti malintenzionati, è importante implementare una serie di azioni preventive.
Ecco alcune delle principali misure di difesa:

1. **Validazione e sanitizzazione dei dati di input:**
   - Verificare e validare tutti i dati di input lato client e lato server assicurandosi che solo i dati validi siano accettati
   - Utilizzare funzioni di sanitizzazione per rimuovere caratteri pericolosi come virgolette, backslashes e caratteri speciali dalle stringhe di input.
2. **Implementazione di un firewall delle applicazioni Web (WAF):**
   - Utilizzare un WAF per filtrare e monitorare il traffico HTTP/HTTPS in ingresso e in uscita, rilevando e bloccando eventuali attacchi XSS o SQLi.
3. **Limitare i privilegi:**
   - Limitare i privilegi di accesso al database per l'applicazione, garantendo che l'account utilizzato per l'accesso al database abbia solo i privilegi necessari per eseguire le operazioni richieste.
4. **Codifica output:**
   - Codificare tutti i dati dinamici in uscita usando tecniche come HTML encoding per prevenire attacchi XSS. Ciò assicura che i dati vengano trattati come dati e non come codice eseguibile.
5. **Controllo header:**
   - Impostare correttamente gli header HTTP, come Content-Security-Policy (CSP), per limitare
   l'esecuzione di script lato client e ridurre il rischio di attacchi XSS.
6. **Aggiornamento e patching:**
   - Mantenere aggiornati tutti i componenti dell'applicazione, inclusi framework, librerie e server
   Web, per mitigare le vulnerabilità conosciute.
7. **Testing di sicurezza:**
   - Condurre regolarmente test di sicurezza, come test di penetrazione e scanner di vulnerabilità, per identificare e correggere eventuali falle di sicurezza.
8. **Monitoraggio e registrazione:**
   - Implementare un sistema di monitoraggio e registrazione per tracciare e analizzare il traffico anomalo o tentativi di attacco.

Impatto sul business

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS, possiamo utilizzare la seguente formula:
Impatto sul business = (Perdita di entrate al minuto) x (Durata dell'interruzione in minuti).

Dato che ogni minuto gli utenti spendono in media 1.500 € sulla piattaforma di e-commerce e l'interruzione dura 10 minuti, possiamo calcolare l'impatto come segue:
Impatto sul business = 1.500 €/minuto x 10 minuti = 15.000 €

Quindi, l'attacco DDoS ha un impatto di perdita di entrate di 15.000 € sul business durante i 10 minuti di non raggiungibilità del servizio.

Per mitigare gli effetti di un attacco DDoS e ridurre l'impatto sul business, è possibile prendere in considerazione le seguenti azioni preventive:

1. Monitoraggio delle prestazioni:
- Implementare sistemi di monitoraggio delle prestazioni dell'applicazione e della rete per identificare tempestivamente anomalie e rispondere prontamente agli attacchi DDoS.

2. Collaborazione con fornitori di servizi:
- Collaborare con fornitori di servizi Internet (ISP) e fornitori di servizi cloud per implementare misure di protezione contro gli attacchi DDoS a livello di rete e mitigare gli effetti di tali attacchi sul servizio.

3. Backup e ripristino dei dati:
- Effettuare regolarmente il backup dei dati critici dell'applicazione e implementare procedure di ripristino rapido per ridurre al minimo il tempo di inattività in caso di attacchi DDoS o altri eventi di perdita di dati.

4. Log SIEM e piattaforme SOAR:

- Utilizzando i dati raccolti, i SIEM possono monitorare il traffico di rete in tempo reale e identificare anomalie che potrebbero indicare un attacco DDoS in corso.
- I SIEM possono correlare gli eventi provenienti da diverse fonti e identificare le relazioni tra di essi per rilevare un possibile attacco DDoS. I SOAR possono automatizzare la risposta avviando azioni predefinite.
- I SIEM possono fornire una piattaforma centralizzata per la gestione dei log e Le piattaforme SOAR possono automatizzare il processo di gestione degli incidenti,

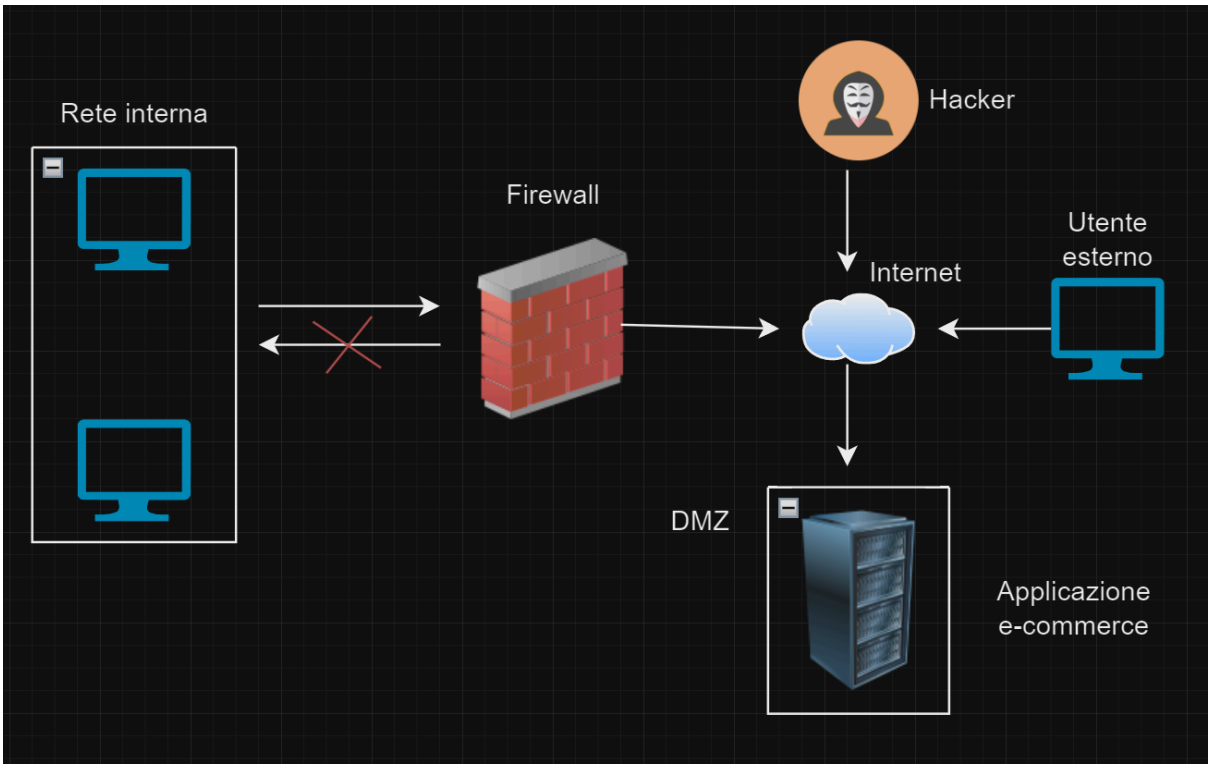
5. Strategia di Disaster recovery:

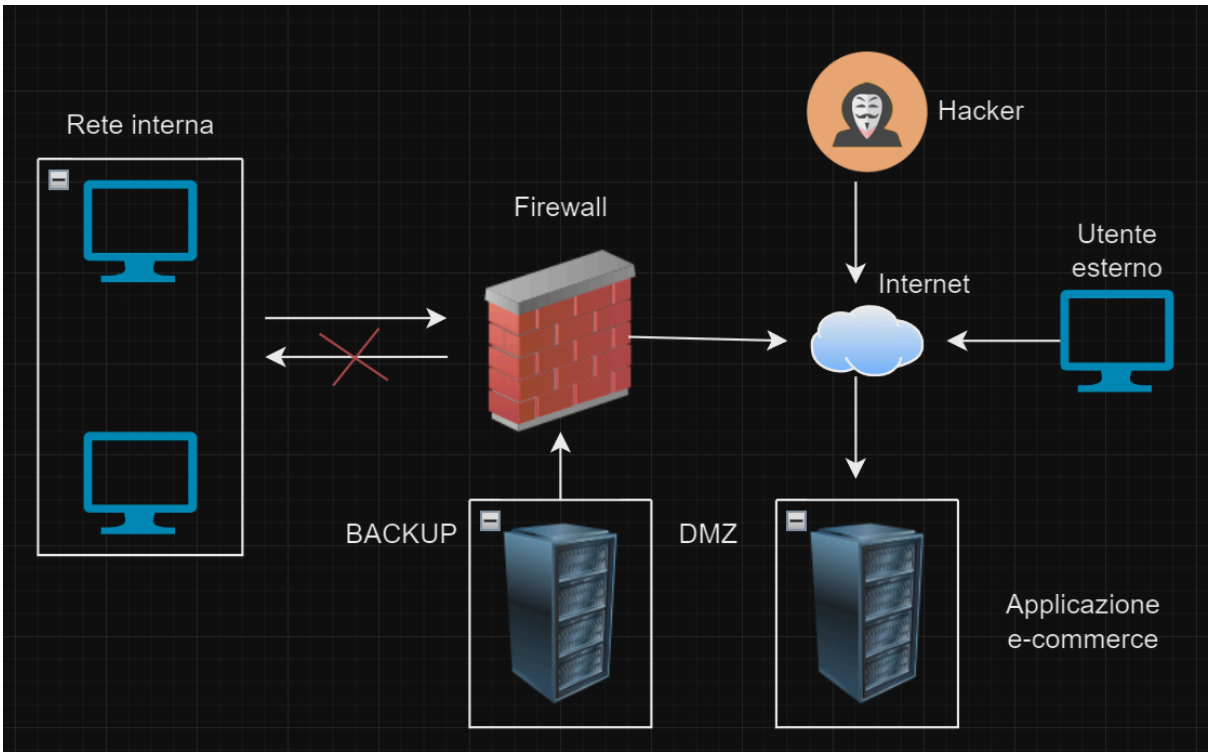
- Mantenere regolari backup dei dati critici dell'azienda in modo che, in caso di interruzione del servizio causata da un attacco DDoS, sia possibile ripristinare rapidamente i dati essenziali e riprendere le operazioni.
- Creare e implementare un piano di continuità aziendale (BCP) che includa procedure per mantenere le operazioni aziendali essenziali durante un attacco DDoS. Questo può includere l'utilizzo di sistemi di backup, l'implementazione di sistemi di ridondanza e la distribuzione di carico su più server.

6. Warm Site:

- Duplicazione dell'infrastruttura critica necessaria per mantenere in funzione il servizio durante un attacco DDoS.
- Quando viene rilevato un attacco, il personale di sicurezza può attivare il sito WARM per mitigare gli effetti dell'attacco e mantenere l'operatività del servizio.
- Stabilire procedure di comunicazione e gestione degli incidenti per coordinare le attività durante un attacco DDoS.

Response





La segmentazione e l'isolamento di una rete sono entrambe pratiche importanti per garantire la sicurezza e l'efficienza delle reti informatiche, ma hanno scopi leggermente diversi e possono essere implementate in modi diversi. In questo caso alla rete è stata applicata una segmentazione, abbiamo eseguito un backup dell'app web e isolato il server principale.

Ecco le differenze principali:

Segmentazione di rete:
La segmentazione di rete suddivide una rete in più segmenti logici o fisici, creando gruppi separati di dispositivi all'interno della rete.
È spesso utilizzata per migliorare l'efficienza del traffico di rete, ottimizzare le prestazioni e semplificare la gestione della rete.

Isolamento di rete:
L'isolamento di rete implica la separazione di parti della rete per impedire o limitare il traffico tra di esse, spesso per ragioni di sicurezza.
È principalmente finalizzato a garantire la sicurezza della rete, proteggendo i dati sensibili e prevenendo la diffusione di minacce informatiche.

Per quanto riguarda i sistemi, server e host, se sono stati compromessi da un attaccante durante un attacco dovrebbero essere considerati non più affidabili e dovrebbero essere di conseguenza ripuliti a fondo prima di essere utilizzati nuovamente.
A tale scopo, si utilizzano le tecniche di «reconstruction» o «rebuilding»
.
• **Reconstruction:** include tutte quelle attività che mirano a recuperare quelle parti ancora affidabili di un sistema compromesso.
• **Rebuilding:** include tutte quelle attività che mirano a ricostruire interamente un sistema impattato considerato non più affidabile.

Per quanto riguarda invece applicazioni, server e software, prima di procedere con la fase di recupero bisogna capire qual è stato il punto di ingresso, per capire dove sono presenti eventuali scoperture di sicurezza per implementare le patch ed evitare che lo stesso incident possa capitare in futuro.

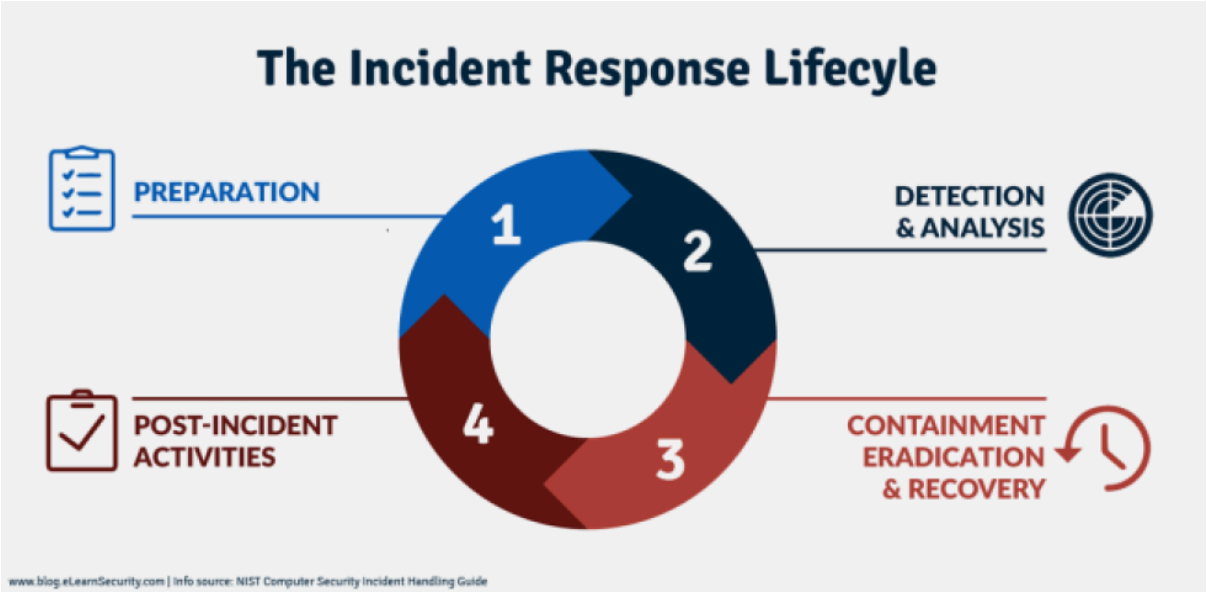
Durante la fase di recupero, ci si trova spesso a dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso.
In questo caso, bisogna accertarsi in prima istanza che le informazioni presenti sul disco/componente siano completamente inaccessibili prima di smaltire/utilizzare nuovamente il disco.
Generalmente, possiamo individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:

• **Clear**: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale;

• **Purge:** si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi:

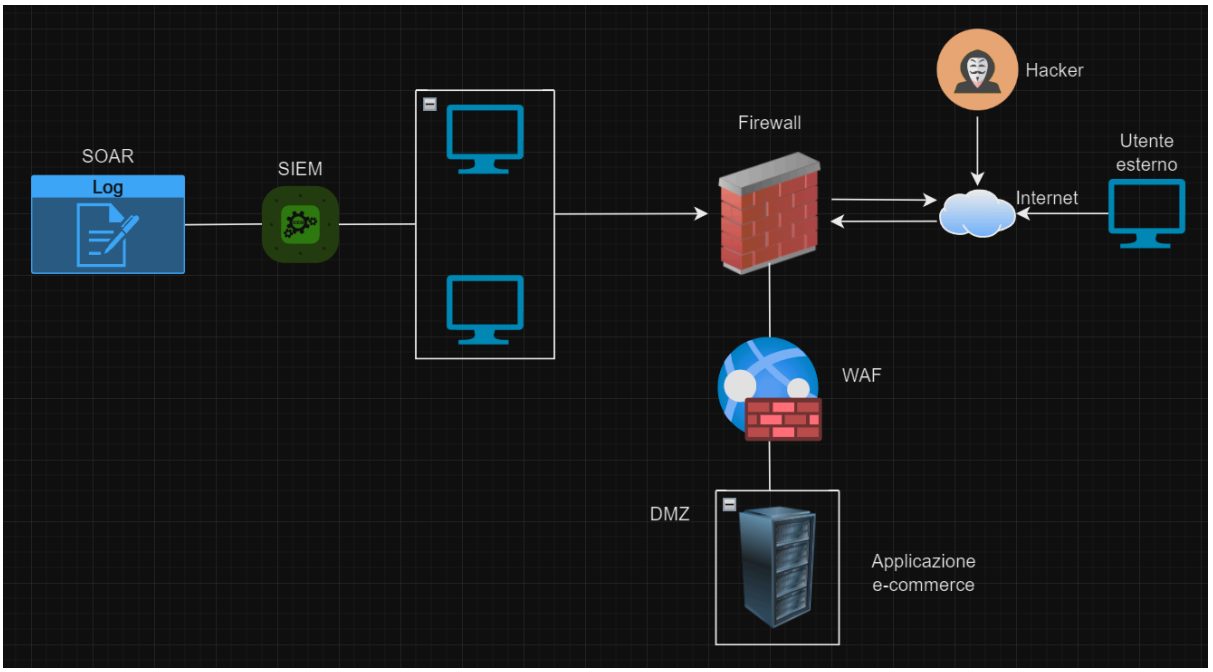
• **Destroy:** è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili.

L'ultima fase di un piano di incident response è la fase **post-incidente** dove si fanno delle considerazioni su cosa poteva esser fatto meglio, cosa poteva esser fatto per evitare determinate situazioni.
Quest'analisi post-incident viene detta «*lesson learnt/learned*», ed è di grande aiuto per imparare dagli errori o da eventuali mancanze che avrebbero potuto evitare l'incidente.



Soluzione completa + modifica

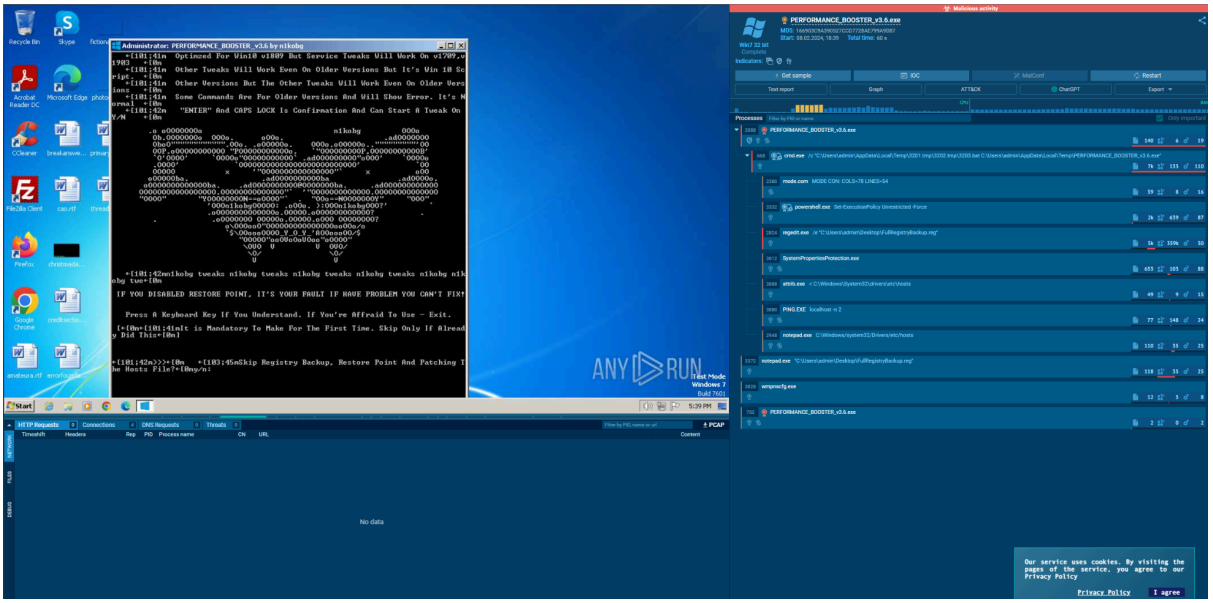
Definiamo quindi la rete finale:



• Internet: Rappresenta la connessione esterna alla rete.
• DMZ (Demilitarized Zone): È una zona intermedia tra la rete interna e Internet, contenente solo l'applicazione.
• Firewall: Serve a proteggere la rete interna e la DMZ controllando il traffico di rete.
• WAF (Web Application Firewall): è un tipo di firewall a livello di applicazione progettato per proteggere le applicazioni Web.
• Utente Esterno: Indica un utente che accede all'applicazione dall'esterno.
• PC Interno #1 e PC Interno #2: Rappresentano i dispositivi all'interno della rete interna.
• SIEM (Security Information and Event Management): È una piattaforma che raccoglie, analizza e interpreta i log di sicurezza e gli eventi da diverse fonti all'interno dell'ambiente IT.
• SOAR (Security Orchestration, Automation, and Response): È una piattaforma che automatizza la risposta agli eventi di sicurezza, coordinando le azioni tra diversi strumenti di sicurezza e accelerando la risposta agli incidenti.

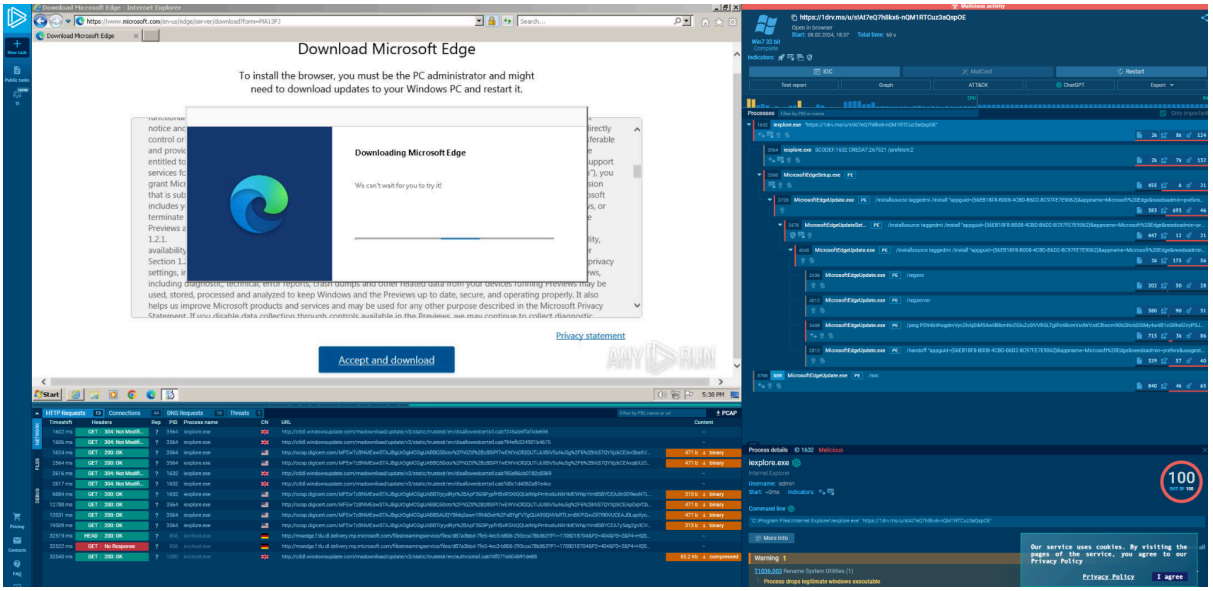
Bonus

• L’esecuzione del file denominato PERFORMANCE_ BOOSTER_V3.6.exe* porta alla creazione di diversi file.
Questo porta a tentativi di aggirare la sicurezza del sistema operativo eseguendo script dannosi per prendere il controllo della macchina ed estrapolare i dati.



Bisogna sempre fare molta attenzione a quello che si esegue e tenere sempre aggiornati i nostri sistemi. Effettuare scansioni periodiche e fare attenzione a scaricare file da siti non sicuri.

• Questo malware si camuffa come un aggiornamento di windows edge. Una volta avviato il download vengono scaricati dei file dannosi che si infiltrano nel sistema andando a manipolare le impostazioni di rete.



Per proteggersi da questi virus è dunque buona norma configurare un WAF (Web Application Firewall) per proteggersi da applicazioni web di questo tipo.

Grazie.

Buonanno Manuel

22/03/2024

EPICODE