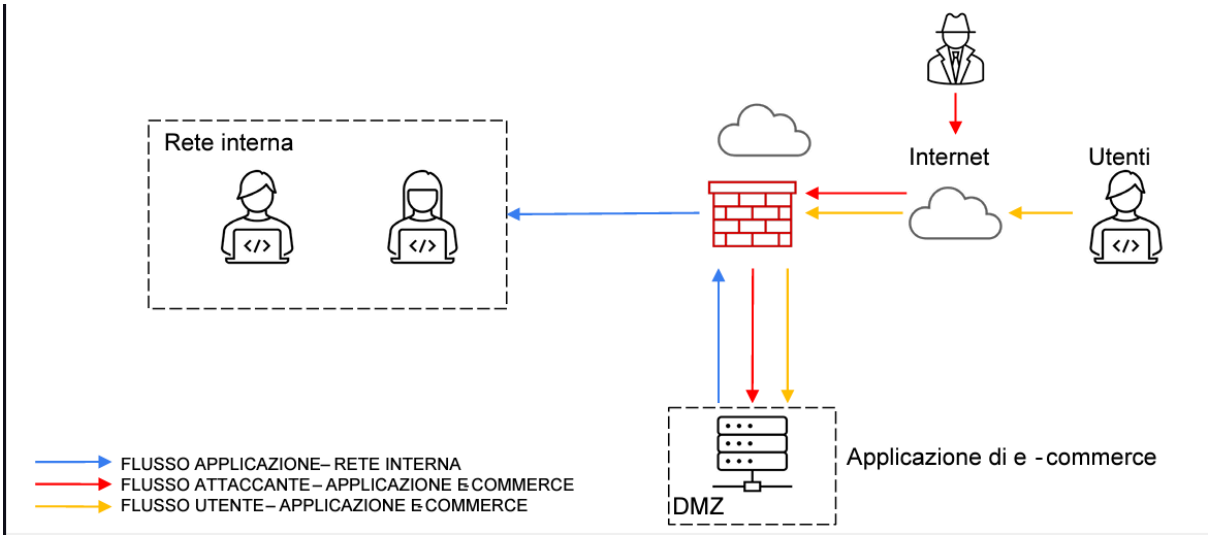
PROGETTO S9/L5

Traccia: con riferimento alla figura in slide 2, rispondere ai seguenti quesiti:

1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQL injection 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 vostre 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).

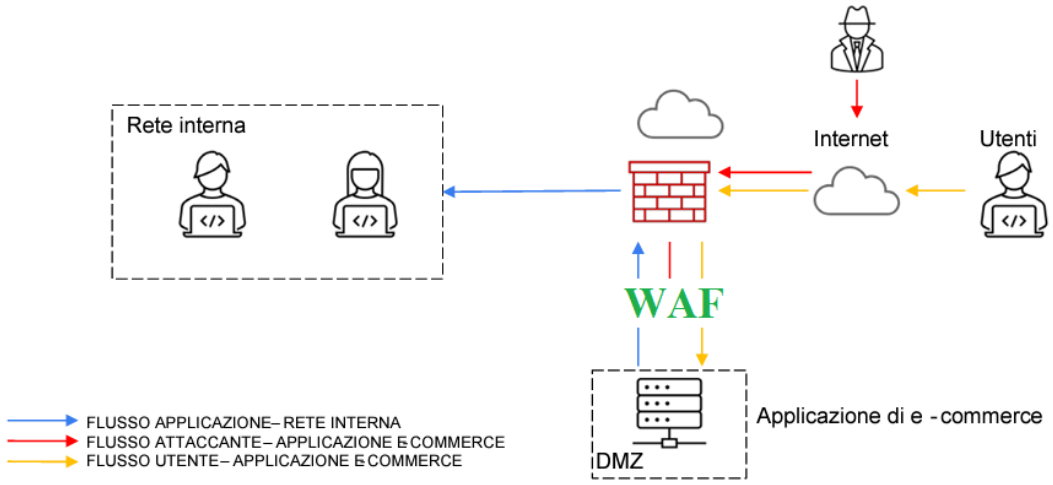
Architettura di rete: l'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Svolgimento:

1. Le **azioni preventive** possono essere viste come l'insieme dei controlli di sicurezza che vengono adottati da una compagnia per aumentare il livello di protezione perimetrale ed interno al fine di ridurre il rischio di potenziali attacchi. In particolare, in questo caso è sicuramente necessario un **Web Application Firewall (WAF)** per proteggere le applicazioni da attacchi quali SQL injection e Cross Site Scripting (XSS). Un Web Application Firewall è un'applicazione o un servizio di sicurezza progettato per proteggere le applicazioni web da attacchi malevoli o indesiderati. Funziona come uno strato di protezione tra l'applicazione

web e il traffico Internet, filtrando e monitorando il traffico HTTP/HTTPS in ingresso e in uscita per identificare e bloccare attacchi mirati alle applicazioni web.



Altre best practices da mettere in pratica potrebbero essere la validazione e sanitizzazione dei dati in input (cioè bisogna assicurarsi che tutti i dati in input forniti dagli utenti siano validati e sanificati correttamente prima di essere utilizzati dall'applicazione), l'utilizzo di prepared statements o parametrized queries per le interrogazioni al database (questo metodo aiuta a prevenire gli attacchi di SQL injection perché separa i dati dalle istruzioni SQL, rendendo impossibile l'inserimento di istruzioni SQL dannose nei dati), l'utilizzo di meccanismi di protezione XSS come Content Security Policy (implementare una CSP può aiutare a mitigare gli attacchi XSS limitando quali risorse possono essere caricate e da dove possono essere caricate), aggiornamento regolare dei software e delle librerie, test periodici di sicurezza per identificare e correggere le vulnerabilità prima che possano essere sfruttate dagli aggressori.

2. Per calcolare l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS, possiamo utilizzare la seguente formula:

Impatto finanziario = (Fatturato medio per minuto) * (Numero di minuti di indisponibilità)

Dato che gli utenti spendono in media 1.500€ sulla piattaforma di e-commerce ogni minuto, possiamo calcolare l'impatto finanziario come segue:

Impatto finanziario = 1.500 €/min * 10 min = 15.000 €

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti sarebbe di 15.000 €. Per quanto riguarda le **azioni preventive** che possono essere implementate per affrontare un attacco DDoS, queste sarebbero quelle necessarie:

- **Implementare una protezione DDoS**: utilizzare servizi di mitigazione DDoS forniti da fornitori di servizi cloud o utilizzare dispositivi dedicati che possano rilevare e mitigare gli attacchi DDoS in tempo reale.
- **Configurare filtri IP**: configurare filtri IP per bloccare o limitare l'accesso a determinati indirizzi IP noti per condurre attacchi DDoS.
- **Backup**: quando si verificano attacchi che causano il crollo del traffico internet o la perdita di dati, è possibile utilizzare i backup per ripristinare i dati e ripristinare il funzionamento normale dei sistemi. Tuttavia, è importante ricordare che i backup devono essere protetti adeguatamente per evitare la loro compromissione da parte

degli attaccanti. Ciò include l'adozione di misure di sicurezza come la crittografia dei dati di backup e la separazione fisica o logica dei backup dai sistemi di produzione.

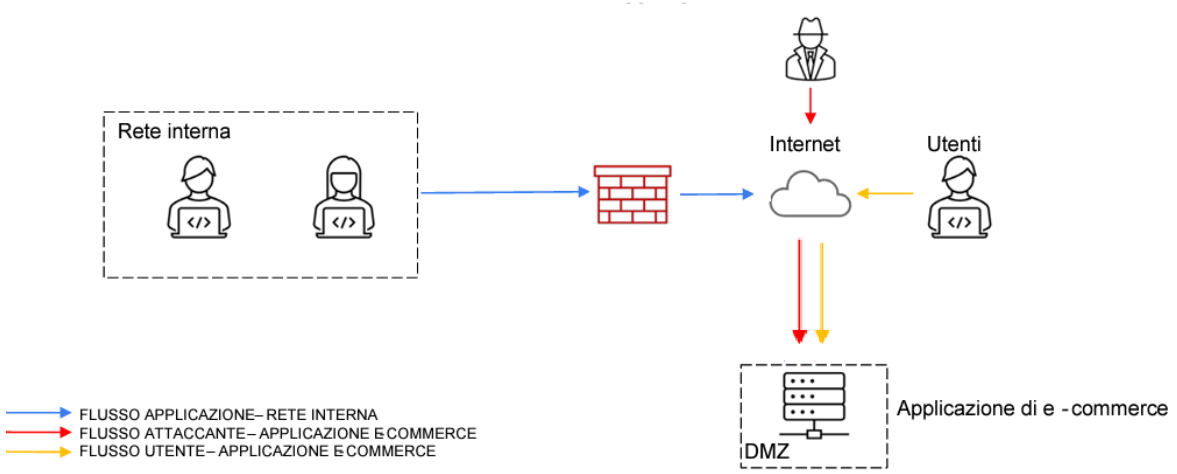
- **Pianificazione di risposta agli incidenti**: avere un piano di risposta agli incidenti ben definito che includa procedure per mitigare gli attacchi DDoS e ripristinare rapidamente la disponibilità del servizio.

Implementando queste azioni preventive, è possibile ridurre significativamente il rischio e l'impatto degli attacchi DDoS sull'applicazione e-commerce.

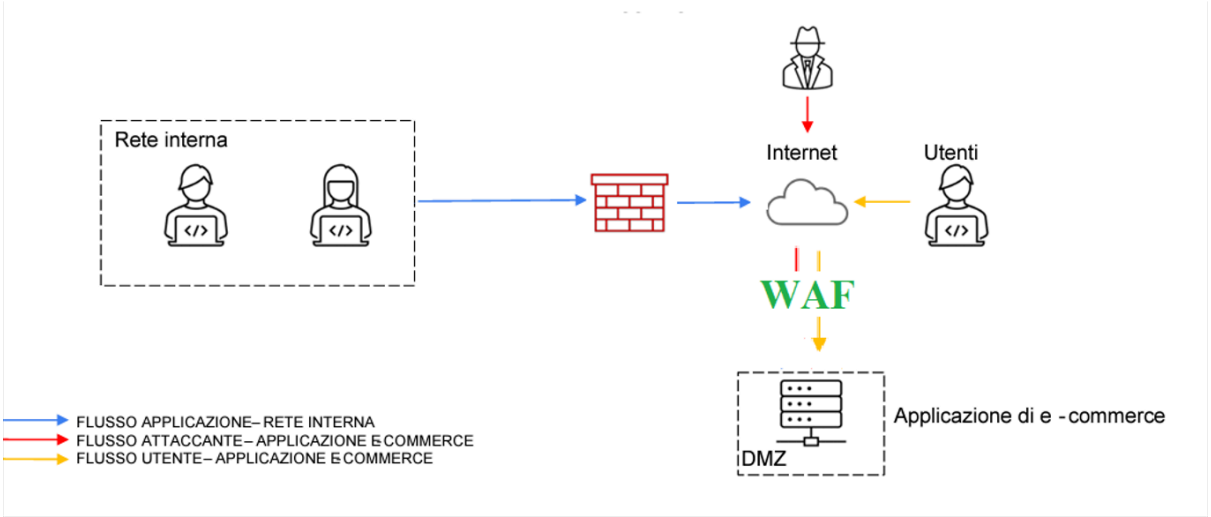
3. Per evitare la propagazione del malware sulla rete interna senza rimuovere immediatamente l'accesso dell'attaccante alla macchina infettata è possibile adottare diverse response, e queste sono quelle che riterrei fondamentali:

- **Isolamento della macchina infetta**: isolare la macchina infetta dalla rete interna utilizzando VLAN, subnet separate o altre tecniche di isolamento di rete. In questo modo si impedisce al malware di propagarsi ad altri dispositivi sulla rete.
- **Monitoraggio del traffico di rete**: implementare strumenti di monitoraggio del traffico di rete per rilevare eventuali tentativi di comunicazione sospetti dalla macchina infetta verso altri dispositivi sulla rete.
- **Analisi del malware**: analizzare il malware per comprendere il suo funzionamento e i suoi comportamenti. Questo può fornire informazioni utili per sviluppare contromisure e rilevare attività sospette sulla rete.

Implementando queste response è possibile limitare la propagazione del malware sulla rete e proteggere gli altri dispositivi dalla compromissione, pur consentendo all'attaccante di mantenere l'accesso alla macchina infettata per scopi di monitoraggio e raccolta di informazioni.



4. L’unione dell’azione preventiva e della response risulta in questa immagine:



5. Una modifica più "aggressiva" dell'infrastruttura potrebbe comportare l'integrazione di elementi di sicurezza più avanzati per migliorare la protezione contro una vasta gamma di minacce informatiche. Ecco alcune opzioni per un'infrastruttura di sicurezza più avanzata:

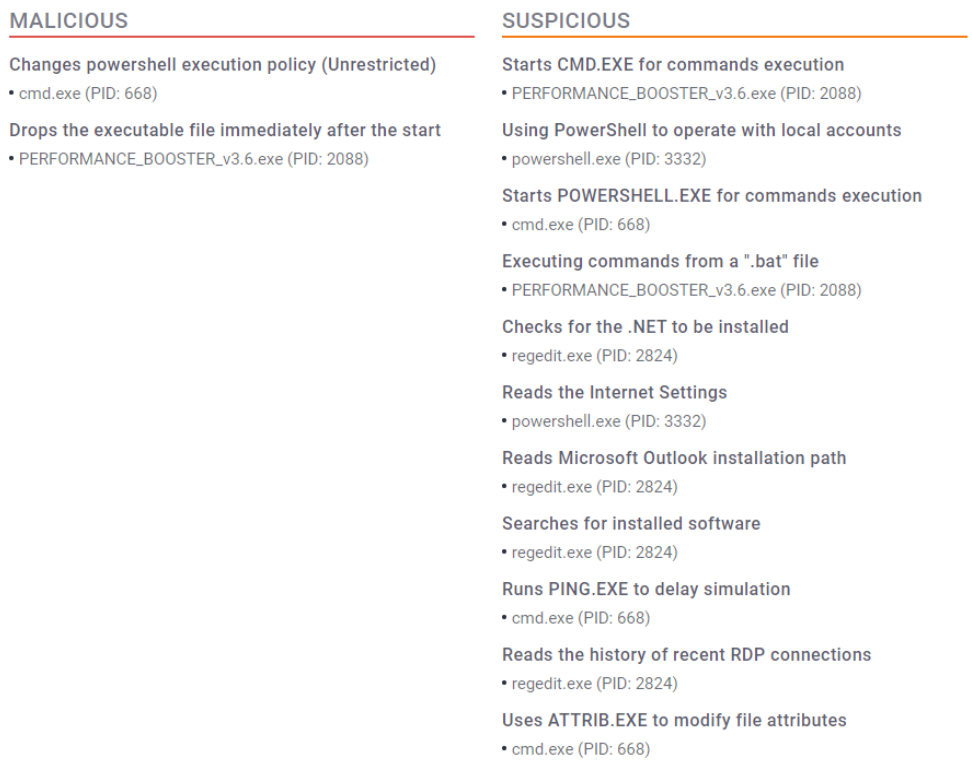
- **Implementare controlli di sicurezza avanzati**: utilizzare soluzioni di sicurezza avanzate come sistemi di rilevamento delle minacce e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere la rete da attività malevole.
- **Sistema di rilevamento e risposta agli incidenti (IDR/IR)**: implementare una soluzione IDR/IR avanzata che monitori costantemente il traffico di rete, i log degli eventi e altri indicatori di compromissione per rilevare tempestivamente le minacce e rispondere prontamente agli incidenti di sicurezza.
- **Analisi comportamentale e machine learning**: utilizzare tecnologie avanzate di analisi comportamentale e machine learning per rilevare pattern anomali e comportamenti sospetti all'interno della rete, consentendo di identificare e rispondere a minacce emergenti in tempo reale.
- **Segmentazione della rete**: implementare una segmentazione della rete più avanzata utilizzando tecniche come micro segmentazione e segmentazione basata su identità per limitare la superficie di attacco e isolare le risorse critiche da potenziali minacce.
- **Autenticazione multi-fattore (MFA)**: estendere l'uso dell'autenticazione multi-fattore per aggiungere un ulteriore livello di sicurezza all'accesso agli applicativi e ai dati sensibili, riducendo così il rischio di accessi non autorizzati.
- **Crittografia end-to-end**: implementare la crittografia end-to-end per proteggere i dati sensibili durante il trasferimento e lo storage, garantendo che siano inaccessibili anche in caso di compromissione della rete o dei dispositivi.
- **Firewall avanzati**: utilizzare firewall avanzati che offrono funzionalità di analisi approfondite del traffico, protezione contro attacchi avanzati come gli attacchi a livello di applicazione e capacità di isolamento delle minacce per ridurre la superficie di attacco e mitigare le violazioni di sicurezza.
- **Protezione degli endpoint avanzata**: implementare soluzioni di protezione degli endpoint avanzate che utilizzano tecniche come l'analisi comportamentale, la protezione delle memorie, e la prevenzione degli exploit per rilevare e bloccare le minacce agli endpoint.

- **Gestione dei privilegi e controllo degli accessi avanzati**: implementare politiche avanzate di gestione dei privilegi e controllo degli accessi per garantire che solo gli utenti autorizzati possano accedere alle risorse e ai dati sensibili, riducendo così il rischio di accessi non autorizzati e di compromissione dei dati.
- **Full backup**: un full backup è un tipo di backup che copre l'intero insieme di dati e file presenti su un sistema o su una determinata porzione di esso. Durante un full backup, vengono copiati tutti i file e i dati selezionati, indipendentemente dal fatto che siano stati modificati dall'ultimo backup o meno. Questo significa che tutti i dati vengono copiati integralmente, senza differenziazioni o riduzioni di dimensione.

Integrare queste tecnologie avanzate di sicurezza nell'infrastruttura può fornire una protezione più completa e resiliente contro una vasta gamma di minacce informatiche, consentendo di rilevare, mitigare e rispondere prontamente alle violazioni di sicurezza in modo più efficace. Queste sono tuttavia delle misure di sicurezza che comportano notevoli costi, quindi non tutte le aziende se le possono permettere e dovranno scegliere quelle che rientrano nel loro budget.

Bonus:
Analizzare le seguenti segnalazioni caricate su anyrune 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/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/
https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

La prima segnalazione riporta una malicious activity che è sostanzialmente un malware che si spaccia per un programma che aumenta le prestazioni del dispositivo, ma in realtà modifica le impostazioni della powershell in modo che possa eseguire linee di comando senza restrizioni, e in questo modo leggere i log di sistema e quelli delle connessioni.



La seconda segnalazione riporta una malicious activity legata al download di microsoft edge: si tratta probabilmente di un cavallo di troia, l'attaccante ha clonato il sito legittimo di edge e ha iniettato del codice malevolo che si scarica automaticamente una volta che l'utente clicca sul bottone download del sito falso. Questo codice malevolo può andare a manomettere il dispositivo operando sulle librerie ddl, in particolare l'attaccante può guadagnare il controllo da remoto del dispositivo e diffondere ulteriori malware.

MALICIOUS

Drops the executable file immediately after the start
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

SUSPICIOUS

Process drops legitimate windows executable
- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Executable content was dropped or overwritten
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

Starts a Microsoft application from unusual location
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Disables SEHOP
- MicrosoftEdgeUpdate.exe (PID: 4040)

Starts itself from another location
- MicrosoftEdgeUpdate.exe (PID: 4040)

Creates/Modifies COM task schedule object
- MicrosoftEdgeUpdate.exe (PID: 4012)

Creates a software uninstall entry
- MicrosoftEdgeUpdate.exe (PID: 4040)

Reads the Internet Settings
- MicrosoftEdgeUpdate.exe (PID: 3408)

Reads settings of System Certificates
- MicrosoftEdgeUpdate.exe (PID: 3408)

Checks Windows Trust Settings
- MicrosoftEdgeUpdate.exe (PID: 3408)

Executes as Windows Service
- MicrosoftEdgeUpdate.exe (PID: 3796)

Reads security settings of Internet Explorer
- MicrosoftEdgeUpdate.exe (PID: 3408)

La prima misura di prevenzione da attuare per evitare incidenti simili sarebbe l'istruzione dei dipendenti sul phishing, in questo modo si evita che essi vadano a scaricare file o applicazioni da fonti non sicure. Poi sicuramente è fondamentale installare un firewall e un proxy per evitare che dei file malevoli entrino nel sistema.