

Roberta Mercadante
DanteNet Solutions

Security Operation Center: Protecting SwissLab

P r e s e n t a t i o n

S9L1-5

Security Operation Center:
Process and procedure

Introduzione

Questa settimana per la parte pratica del corso, ci è stato richiesto di definire un'azienda a cui forniremo servizi (in base alle tracce quotidiane degli esercizi) che rimarrà l'azienda da cui saremo ingaggiati per tutta la settimana.

Ci è stata data la possibilità di lavorare in gruppo o in autonomia, e per questo progetto ho deciso di lavorare da sola così da mettermi alla prova sotto ogni aspetto che il compito prevede.

Per la consegna iniziale ho definito due aziende:

- DanteNet solutions azienda incaricata
- SwissLab azienda cliente

Overview

- Introduzione aziende
- Preventivo
- Firewall: impatto su una scansione Nmap
- Business Continuity & Disaster Recovery
- Threat Intelligence e IOC
- Wireshark:
individuazione IOC
- Findings & solutions
- Incident Response
- Architettura di Rete: risposta ai quesiti L5

Intro DanteNet Solutions

DanteNet Solutions S.r.l. è un'azienda specializzata nella fornitura di servizi di sicurezza informatica per imprese di medie e grandi dimensioni.

L'azienda si occupa di proteggere le infrastrutture IT dei clienti attraverso una combinazione di consulenza, implementazione di soluzioni di sicurezza e monitoraggio continuo. I servizi offerti includono:

- Valutazione della Sicurezza di Rete: Analisi e verifica della sicurezza delle reti aziendali per identificare vulnerabilità e rischi potenziali.
- Implementazione di Firewall e Sistemi di Prevenzione delle Intrusioni (IPS): Configurazione e gestione di firewall e sistemi IPS per proteggere le reti da accessi non autorizzati e attacchi.
- Penetration Testing: Test di penetrazione per simulare attacchi reali e identificare punti deboli nel sistema di sicurezza.
- Monitoraggio e Risposta agli Incidenti: Monitoraggio continuo delle reti e risposta immediata agli incidenti di sicurezza per minimizzare i danni.
- Formazione sulla Sicurezza: Programmi di formazione per il personale aziendale per aumentare la consapevolezza e le competenze in materia di sicurezza informatica.

Intro SwissLab

SwissLab S.p.A. è una società leader nel settore medico e delle biotecnologie, specializzata nelle analisi di laboratorio sul DNA e nelle tecnologie avanzate di ricerca medica con una solida reputazione a livello internazionale grazie alla sua eccellenza nella ricerca e nello sviluppo di soluzioni innovative per la diagnosi e il trattamento delle malattie genetiche.

SwissLab S.p.A. rappresenta una realtà all'avanguardia nel settore medico e biotecnologico, con un forte impegno verso l'innovazione e la qualità.

L'azienda offre servizi cruciali per la diagnosi e il trattamento delle malattie genetiche, supportando la comunità medica e scientifica nella diagnosi e nel trattamento dei pazienti, oltre che collaborare con diverse università in tutto il mondo.



L1 Traccia

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.

Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L' esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.

Preventivo #1024

DanteNet Solution S.r.l

Via xxxx Milano, Italia

P.IVA: xxxxxxxxxxxxxxxxxx

Cliente:

SwissLab S.p.A.

Via xxxxxx, Mendrisio, Svizzera

P.IVA xxxxxxxxxxxxxxxxxxxx

Attività	Ore Stimate	Tariffa Oraria 2 specialisti	Costo Totale (€)
Disabilitazione e Abilitazione del Firewall Esecuzione scansioni con Nmap. Redazione e Presentazione di un Report	35	200	7.000
Analisi e Raccolta Dati Sviluppo del Business Continuity and Disaster Recovery Plan Revisione del Piano Formazione Documentazione e Consegna del Piano	130	200	26.000
Cattura di rete con Wireshark Configurazione Analisi Documentazione	20	200	4.000
Incident Response Isolamento Sanificazione Ripristino	30	200	6.000
Progettazione Infrastruttura di Rete	60	200	12.000
		Subtotale	55.000
		Iva	14.300
		Totale	69.300

Termini e condizioni

- Il pagamento sarà effettuato al completamento di ciascuna fase del progetto, secondo le ore effettivamente lavorate.
- Eventuali costi aggiuntivi per materiali o risorse esterne non inclusi nel preventivo saranno discussi e approvati con il cliente prima di essere sostenuti.
- Le modifiche al progetto originale che richiedono ore di lavoro aggiuntive saranno fatturate separatamente.

Accettazione del Preventivo

Firma del Cliente: _____

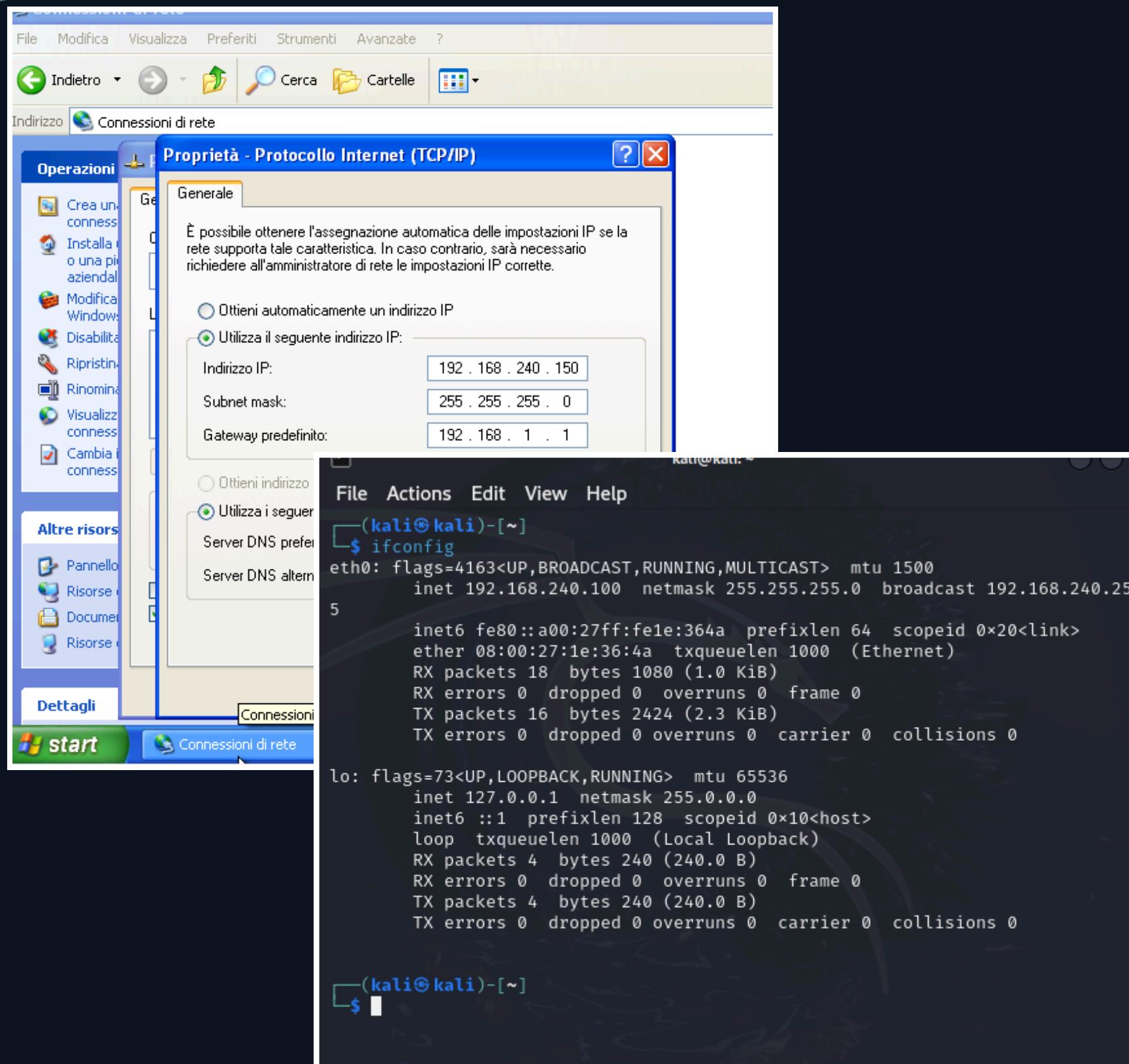
Data: _____

NB: IL PREVENTIVO INCLUDE I SERVIZI

RICHIESTI NELLE TRACCE DA S9L1 A S9L5

S9L1-5

Objectives & Requirements



L'obiettivo dell'esercizio di oggi è quello di verificare come l'attivazione del firewall su una macchina Windows XP impatti i risultati di una scansione dei servizi effettuata dall'esterno utilizzando Nmap.

Come primo passaggio per lo svolgimento di questo esercizio, ho assegnato gli indirizzi IP richiesti alle due macchine.

Avremo quindi come da immagine Windows XP con indirizzo IP: 192.168.240.150 Kali con indirizzo IP: 192.168.240.100.

Scansione Nmap

Prima di procedere con qualsiasi comando, ho verificato che il firewall di Windows XP fosse disabilitato ed ho quindi eseguito la prima scansione nmap utilizzando il comando

`nmap -sV 192.168.240.150`

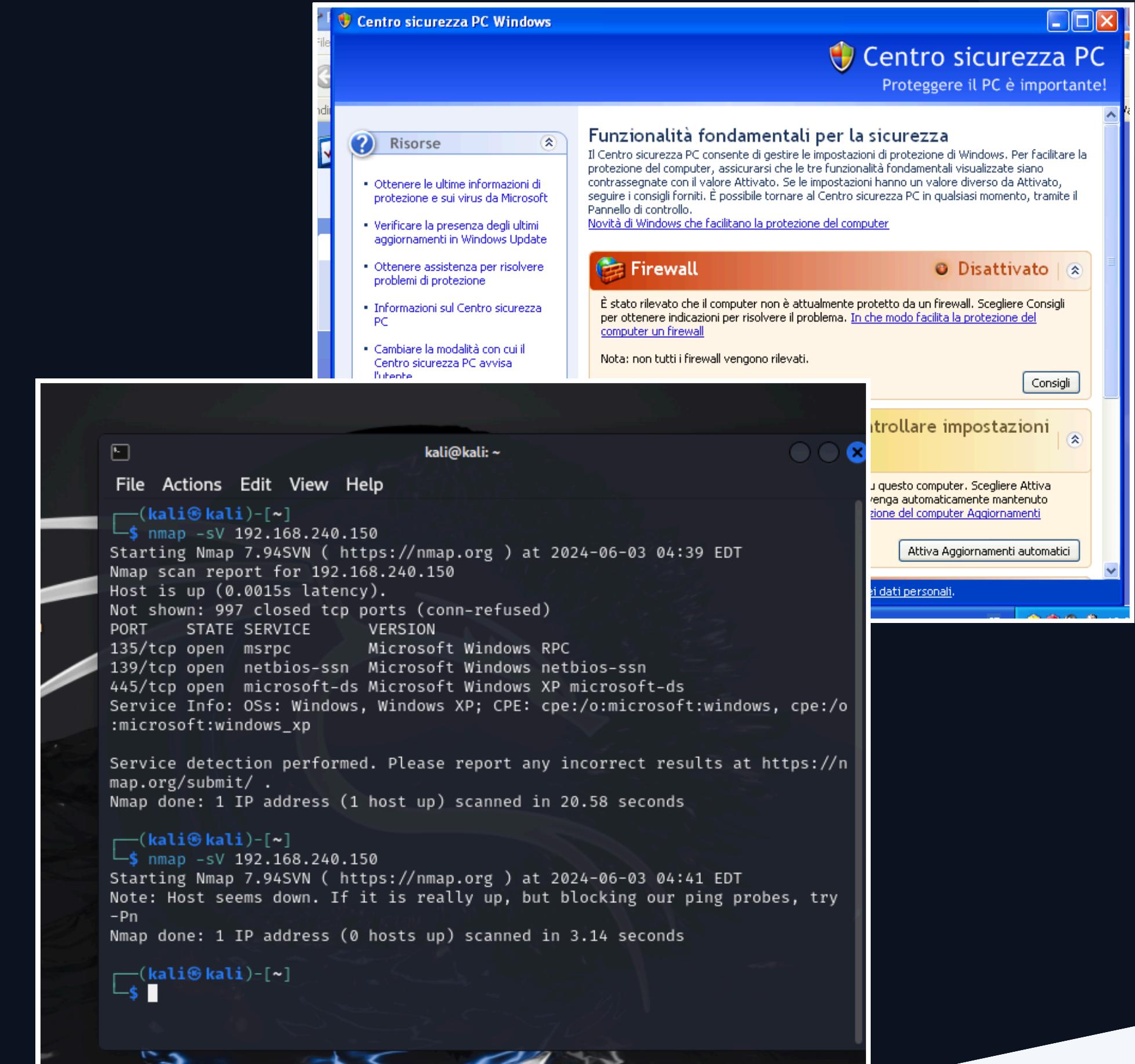
da Kali Linux per effettuare una service detection.

La scansione con il firewall disattivato ha rilevato 3 servizi in ascolto sulle seguenti porte TCP:

Porta 135: servizio Microsoft RPC

Porta 139: servizio NetBIOS-SSN

Porta 445: servizio Microsoft-DS



What happened?



Tornando al pannello di controllo su Windows XP, dal centro sicurezza attivo il firewall.

Eseguo nuovamente la scansione con Nmap utilizzando il comando
nmap -sV 192.168.240.150
da Kali Linux.

La scansione riporta che la macchina o non è accesa, oppure sta bloccando l'host discovery di Nmap.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:41 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds
```

```
(kali㉿kali)-[~]
$
```

Any change?

Utilizzo quindi il comando
nmap -sV -Pn 192.168.240.150
per saltare il ping e passare direttamente
alla service discovery.

La scansione indica che tutte le porte
sembrano filtrate e non hanno risposto alle
richieste dello scanner.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:43 EDT
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.29 seconds

(kali㉿kali)-[~]
└─$
```

Conclusioni

S9L1-5

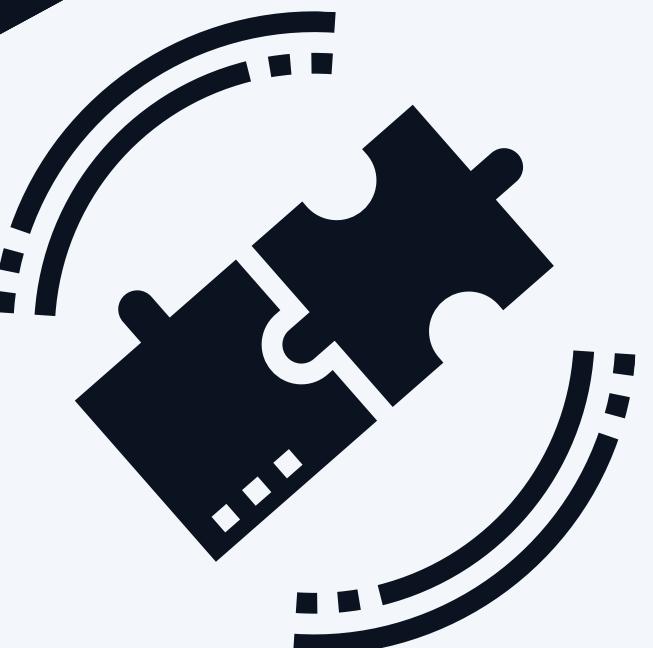
L'attivazione del firewall su una macchina Windows XP ha un impatto significativo sui risultati di una scansione dei servizi effettuata con Nmap.

Con il firewall disattivato, Nmap è stato in grado di rilevare tre servizi attivi sulle porte TCP 135, 139 e 445. Tuttavia, una volta attivato il firewall, la macchina ha bloccato l'host discovery di Nmap, rendendo impossibile la rilevazione dei servizi.

Utilizzando l'opzione -Pn, che forza Nmap a saltare il ping e procedere direttamente alla scoperta dei servizi, tutte le porte sono risultate filtrate.

Questo indica che il firewall sta bloccando attivamente il traffico in ingresso, non rispondendo alle richieste di Nmap.

Questi risultati dimostrano l'efficacia del firewall di Windows XP nel bloccare tentativi di scansione esterna, aumentando significativamente la sicurezza della macchina contro possibili attacchi. L'attivazione del firewall è quindi una misura preventiva cruciale per proteggere i sistemi da traffico potenzialmente dannoso.





L2 Traccia

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery.

Nell' esempio pratico di oggi, ipotizziamo che SwissLab ci abbia assunti anche per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia.

Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
 - Terremoto sull'asset «datacenter»
 - Incendio sull'asset «edificio primario»
 - Incendio sull'asset «edificio secondario»
 - Inondazione sull'asset «edificio primario»

Dati forniti



EPICODE
Business continuity & disaster recovery

Esercizio

Dati:

ASSET	VALORE	EVENTO	ARO
Edificio primario	350.000€	Terremoto	1 volta ogni 30 anni
Edificio secondario	150.000€	Incendio	1 volta ogni 20 anni
Datacenter	100.000€	Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

4

Per valutare quantitativamente l'impatto di un disastro su un asset di una compagnia e calcolare la perdita annuale attesa, utilizziamo il concetto di Annual Loss Expectancy (ALE).

L'ALE viene calcolata come il prodotto tra la probabilità annuale dell'evento e la perdita attesa per evento (Single Loss Expectancy, SLE).

La formula per la SLE è:

$$\text{SLE} = \text{valore dell'asset} * \text{exposure factor (EF)}$$

La formula per la ALE è:

$$\text{ALE} = \text{SLE} * \text{ARO (Annualized Rate of Occurrence)}$$

Procedimento

S9L1-5

Calcoli

Ricordando che: $1/50 = 0,02$; $1/20 = 0,05$; $1/30 = 0,0333$

- Inondazione sull'asset "edificio secondario"

- $SLE = 150.000 \text{ €} * 40\% = 60.000 \text{ €}$
 - $ARO = 1/50$
 - $ALE = 60.000 \text{ €} * (1/50) = 1.200 \text{ €}$

- Terremoto sull'asset "datacenter"

- $SLE = 100.000 \text{ €} * 95\% = 95.000 \text{ €}$
 - $ARO = 1/30$
 - $ALE = 95.000 \text{ €} * (1/30) = 3.163 \text{ €}$

- Incendio sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 60\% = 210.000 \text{ €}$
 - $ARO = 1/20$
 - $ALE = 210.000 \text{ €} * (1/20) = 10.500 \text{ €}$

- Incendio sull'asset "edificio secondario"

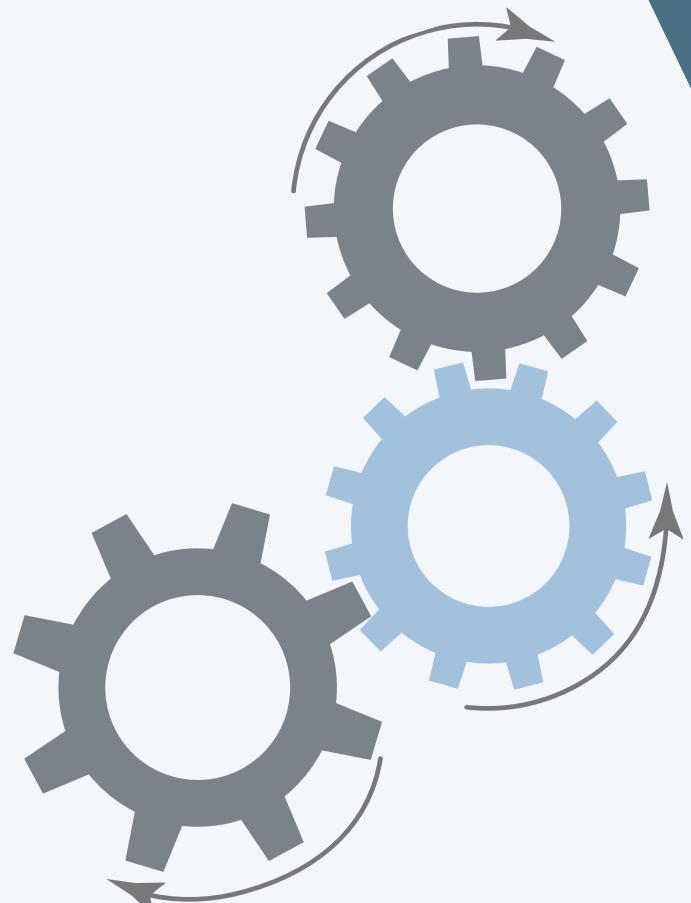
- $SLE = 150.000 \text{ €} * 50\% = 75.000 \text{ €}$
 - $ARO = 1/20$
 - $ALE = 75.000 \text{ €} * (1/20) = 3.750 \text{ €}$

- Inondazione sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 55\% = 192.500 \text{ €}$
 - $ARO = 1/50$
 - $ALE = 192.500 \text{ €} * (1/50) = 3.850 \text{ €}$

- Terremoto sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 80\% = 280.000 \text{ €}$
 - $ARO = 1/30$
 - $ALE = 280.000 \text{ €} * (1/30) = 9.324 \text{ €}$



Business Continuity and Disaster Recovery Plan (BCDRP)

Compagnia: SwissLab S.p.A.

Data: 4 Giugno 2024

Questo piano descrive le procedure per garantire la continuità operativa e il ripristino delle attività aziendali in caso di disastro che colpisca gli asset critici della compagnia SwissLab S.p.A. Il piano è stato sviluppato per mitigare i rischi associati a inondazioni, terremoti e incendi.

Introduzione

- Garantire la continuità delle operazioni critiche di ricerca e sviluppo.
- Proteggere i campioni biologici, i dati clinici e le attrezzature sensibili.
- Ridurre al minimo l'impatto finanziario di disastri su asset chiave.
- Stabilire procedure di risposta e ripristino efficienti per la sicurezza dei pazienti e dei dati.

Obiettivi

Asset Critici e Valutazione dei Rischi

Asset	Valore (€)	Tipo di Evento	Probabilità (ARO)	Exposure Factor (EF)	Single Loss Expectancy (SLE) (€)	Annual Loss Expectancy (ALE) (€)
Edificio primario	350.000	Inondazione	1/50	55%	192.500	3.850
Edificio primario	350.000	Terremoto	1/30	80%	280.000	9.324
Edificio primario	350.000	Incendio	1/20	60%	210.000	10.500
Edificio secondario	150.000	Inondazione	1/50	40%	60.000	1.200
Edificio secondario	150.000	Incendio	1/20	50%	75.000	3.750
Datacenter	100.000	Terremoto	1/30	95%	95.000	3.163

Strategie di Mitigazione

Inondazione:

- Installazione di sistemi di drenaggio e pompe per prevenire accumuli d'acqua.
- Elevazione di laboratori critici e magazzini di campioni biologici al di sopra del livello di inondazione previsto.
- Utilizzo di contenitori ermetici per la conservazione dei campioni biologici.
- Implementazione di barriere contro le inondazioni intorno all'edificio.
- Monitoraggio e allerta precoce per eventi meteorologici estremi.

Terremoto:

- Rafforzamento strutturale dell'edificio per resistere a scosse sismiche.
- Sistemi di scaffalature antisismiche per le attrezzature e i reagenti chimici.
- Implementazione di sistemi di protezione delle apparecchiature IT contro i terremoti.
- Backup regolari dei dati clinici e di ricerca in siti remoti e cloud.
- Sistemi di ridondanza per garantire la disponibilità continua dei dati.

Incendio:

- Installazione di sistemi antincendio avanzati, inclusi sprinkler e rilevatori di fumo.
- Formazione del personale in tecniche di evacuazione e uso di estintori.
- Protocollo di sicurezza per il trattamento di materiali infiammabili e reattivi.
 - Sistemi di rilevazione e soppressione del fuoco.
- Regolare manutenzione e ispezione degli impianti elettrici e delle attrezzature.
- Procedure di emergenza per la manipolazione di sostanze pericolose.

Rischi di Cybersecurity in Caso di Disastri Naturali

Perdita di Dati e Sistemi

Danni fisici ai server, ai data center e ai dispositivi di archiviazione che possono portare alla perdita di dati critici.

Perdita permanente di dati importanti, interruzione delle operazioni aziendali, compromissione della ricerca e sviluppo.

Accesso Fisico Non Autorizzato

Durante un disastro, le misure di sicurezza fisica possono essere compromesse, permettendo l'accesso non autorizzato ai sistemi e ai dati.

Furto di dati sensibili, alterazione o distruzione di informazioni, esposizione a minacce interne ed esterne.

Interruzione delle Comunicazioni e Controlli di Sicurezza

Interruzioni delle reti di comunicazione e dei sistemi di controllo di sicurezza possono lasciare i sistemi vulnerabili ad attacchi.

Inabilità a monitorare e rispondere a minacce in tempo reale, aumentando il rischio di attacchi informatici durante il disastro.

Corruzione dei Dati

Danneggiamento fisico o corruzione dei dati a causa di disastri naturali può compromettere l'integrità delle informazioni.

Dati danneggiati o alterati possono portare a decisioni errate, compromissione della qualità della ricerca e perdita di fiducia da parte dei clienti e dei partner.

Strategie di Mitigazione legate alla cybersecurity

Backup e Ripristino dei Dati

Implementazione di backup regolari, archiviati in sedi diverse e nel cloud, per garantire la disponibilità dei dati anche in caso di disastri fisici.

Sicurezza Fisica e Accesso Controllato

Rafforzamento delle misure di sicurezza fisica nei data center e nei laboratori, videosorveglianza, sistemi di allarme e controlli di accesso ad autenticazione a più fattori.

Ridondanza e Alta Disponibilità

Progettazione di infrastrutture IT ridondanti per garantire la continuità operativa anche in caso di guasti fisici.

Piani di Continuità Operativa e Recupero di Emergenza

Sviluppo di piani di disaster recovery specifici per la ripresa dei sistemi IT e mantenere operazioni critiche durante e dopo un disastro.

Formazione e Sensibilizzazione del Personale

Educazione continua del personale sulle procedure di emergenza, la sicurezza dei dati e le pratiche di cybersecurity durante i disastri.

Monitoraggio e Risposta agli Incidenti

Costituzione di un team dedicato di risposta agli incidenti con protocolli chiari per la gestione delle emergenze di cybersecurity.

Piano di ripristino

- **Attivazione del Team di Risposta ai Disastri:**

Composto da rappresentanti IT, sicurezza, gestione edifici, direzione e responsabili di laboratorio.

Coordinamento con le autorità locali, i servizi di emergenza e le agenzie di regolamentazione.

- **Valutazione del Danno:**

Ispezione immediata degli asset colpiti per determinare l'entità del danno.

Documentazione dei danni per la successiva richiesta di indennizzo assicurativo.

Messa in sicurezza dei campioni biologici e dei dati sensibili.

- **Ripristino Temporaneo:**

Trasferimento delle operazioni critiche di laboratorio in strutture alternative, se necessario.

Attivazione di backup dati e sistemi IT in siti remoti.

Controllo della qualità e dell'integrità dei campioni biologici.

- **Ripristino Completo:**

Riparazione e ristrutturazione degli asset danneggiati.

Verifica e test dei sistemi ripristinati prima del ritorno alle operazioni normali.

Validazione della qualità dei processi e dei prodotti di laboratorio.

Comunicazione

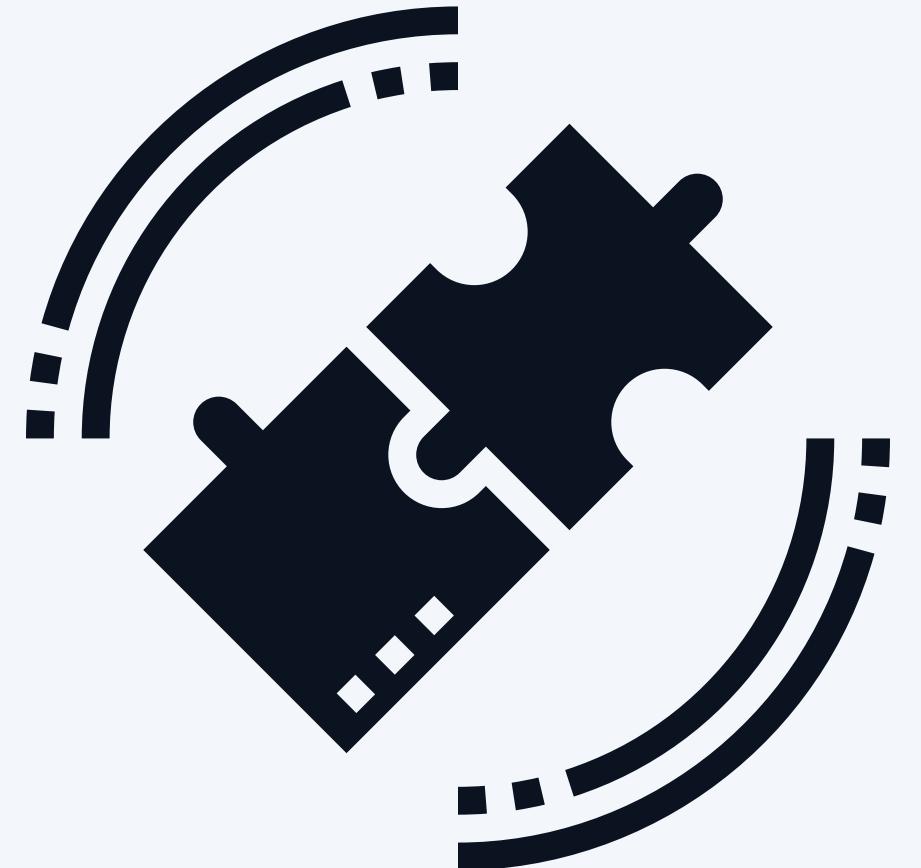
Interna:

- Aggiornamenti regolari al personale sull'avanzamento del ripristino.
- Canali di comunicazione di emergenza (e-mail, messaggi, bacheche aziendali).

Esterna:

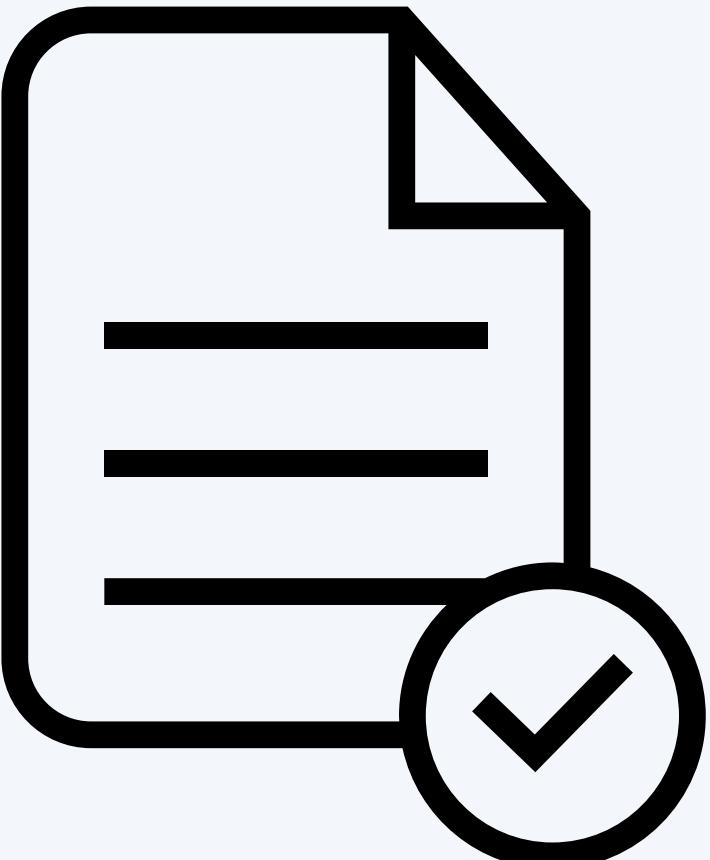
- Comunicazione con clienti, fornitori, partner di ricerca e altre parti interessate.
- Utilizzo di comunicati stampa e aggiornamenti sui social media per informare il pubblico e le agenzie di regolamentazione.
- Comunicazione con le autorità sanitarie e regolatorie in caso di impatti sui dati clinici o sulla ricerca.

S9L1-5



Formazione e Test

- Programmi di formazione regolari per il personale su procedure di emergenza e sicurezza.
- Addestramento specifico per la manipolazione sicura di campioni biologici e reagenti pericolosi.
- Simulazioni di disastro e prove di evacuazione per verificare l'efficacia del piano.
- Revisione e aggiornamento del piano sulla base dei risultati dei test e dei feedback ricevuti.
- Valutazioni periodiche della conformità alle normative di sicurezza e di qualità.



Manutenzione del piano

Il Business Continuity and Disaster Recovery Plan sarà riesaminato e aggiornato annualmente o in seguito a modifiche significative nelle operazioni aziendali, nell'infrastruttura o nel profilo di rischio. La revisione includerà l'analisi dei cambiamenti nelle normative del settore medico e biotecnologico.





L3 Traccia

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso.
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

What's Wireshark?

Nell' esercizio di oggi abbiamo analizzato una cattura di rete effettuata con Wireshark, che, come sappiamo, è uno strumento di analisi del traffico di rete che consente di catturare e visualizzare i dati trasmessi su una rete in tempo reale. Le evidenze raccolte da Wireshark possono essere utili per una vasta gamma di scopi, tra cui il troubleshooting di problemi di rete, l'analisi della sicurezza e la verifica della conformità. Le evidenze più comuni che Wireshark può fornire sono appunto la cattura del traffico di rete, le informazioni sui pacchetti, i dettagli sulle sessioni TCP e UDP, analisi del traffico HTTP, DNS e SSL, analisi di attacchi come tentativi di exploit, attacchi DDoS e scansioni delle porte, flag TCP anomali e molto altro.

IOC

Nello specifico, l'esercizio di oggi, chiede di identificare eventuali IOC. Iniziamo ricordando che gli Indicatori di Compromissione (IOC), sono evidenze o tracce che indicano che un sistema di informazione o una rete potrebbero essere stati compromessi da un attacco informatico. In parole semplici, sono come "impronte digitali" che i criminali informatici lasciano dietro di sé e che possono aiutare gli esperti di sicurezza a rilevare e rispondere a tali attacchi.

Negli screenshot che seguono andremo ad analizzare la cattura di rete effettuata con wireshark e dopo aver identificato eventuali IOC, l' esercizio chiede di ipotizzare i potenziali vettori di attacco e consigliare un azione per ridurre gli impatti dell'attacco.



Cattura di Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

0000 ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00 E
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8 &

Analisi

Dallo primo screen possiamo notare che il primo pacchetto mostra un annuncio host per "METASPLOITABLE". Metasploitable come sappiamo è una macchina virtuale utilizzata comunemente per test di penetrazione e potrebbe indicare che ci sia una sessione di test di penetrazione o un attacco in corso. Dallo screen possiamo anche vedere che ci sono numerosi pacchetti TCP con flag RST e questo potrebbe indicare che la connessione è stata interrotta bruscamente, un comportamento che potrebbe essere associato a un attacco DoS (Denial of Service).

Ci sono anche numerosi pacchetti SYN senza un corrispondente ACK che potrebbero indicare un tentativo di SYN flood, che è un tipo di attacco DoS volto a esaurire le risorse di connessione di un server. Ci sono anche pacchetti ARP che cercano di risolvere molti indirizzi in un breve lasso di tempo e questo lascia spazio all' ipotesi di uno scanning della rete che un attaccante potrebbe utilizzare per mappare i dispositivi connessi.

Le azioni che si potrebbero compiere per ridurre l'impatto degli attacchi sono innanzi tutto di configurare un firewall con regole più restrittive così da limitare il traffico in entrata e in uscita, aumentare il monitoraggio della rete in tempo reale così da rispondere prontamente ad eventuali attacchi. Inoltre, è sempre buona abitudine mantenere i software e i dispositivi aggiornati così da ridurre la presenza di vulnerabilità fruttabili da un attaccante ed ovviamente formare il personale in modo che sia in grado di riconoscere anomalie o attività sospette.

Cattura di Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776482588	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478281	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33286 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535448 TSecr=0 WS=128
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535448 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	508 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33842 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Analisi

In questo secondo screen, continuano ad esserci molti pacchetti TCP con flag RST/ACK tipici di attacchi DoS e pacchetti SYN senza corrispondenza ACK che possono come scritto sopra indicare appunto tentativi di SYN flood.

Inoltre, la ripetizione di traffico verso specifiche porte TCP potrebbe indicare uno scanning di porta o un tentativo di sfruttare una vulnerabilità nota su quelle porte.

Ad esempio, le porte 80 e 443 potrebbero indicare tentativi di exploit su server web o tentativi di forza bruta su applicazioni web. La porta 445 invece potrebbe indicare probabili tentativi di exploit SMB come EternalBlue, noto per essere utilizzato in attacchi ransomware. La porta 22 possibili tentativi di forza bruta su SSH o exploit di vulnerabilità specifiche del server SSH.

Per mitigare gli effetti di questi attacchi, oltre ad implementare quello scritto sopra, si può limitare il numero di tentativi di connessione da un singolo ip e di connessioni simultanee per cercare di prevenire attacchi DoS. Si consiglia poi utilizzare SYN cookies per gestire le connessioni incomplete. Le SYN cookies sono una tecnica utilizzata per proteggere i server dagli attacchi SYN flood, che sono un tipo di attacco Denial of Service.

Quando un client vuole stabilire una connessione TCP con un server, utilizza il Three Way Handshake, ovvero il client invia un pacchetto SYN al server per avviare la connessione, il server risponde con un pacchetto SYN-ACK comunicando che ha ricevuto la richiesta ed è pronto a ricevere ed il client risponde con un pacchetto ACK completando così il Three Way Handshake e stabilendo la connessione.

In un attacco SYN flood, un attaccante invia un gran numero di pacchetti SYN al server, ma non completa mai l'handshake. Il server riserva risorse per ogni richiesta in attesa della risposta finale ovvero l'ACK, e quando ne arrivano troppe, può esaurire le risorse disponibili, bloccando le connessioni legittime. I SYN cookies aiutano a prevenire questo problema gestendo in modo diverso le richieste di connessione; ovvero quando il server riceve un pacchetto SYN da un client, invece di riservare immediatamente le risorse, crea un SYN cookie, che è un valore hash generato utilizzando alcune informazioni della connessione come l'indirizzo ip del client, la porta del client e un valore segreto del server e lo invia indietro al client come parte del pacchetto SYN-ACK. Se il client è legittimo e risponde con un pacchetto ACK, include il SYN cookie che il server ha inviato. Il server può verificare il SYN cookie senza dover riservare risorse in anticipo ed una volta verificato il SYN cookie, il server può allocare le risorse necessarie per la connessione e procedere con l'handshake.

Tornando all' analisi dello screen sopra, un'altra azione da compiere può essere quella di bloccare gli indirizzi IP che mostrano comportamenti sospetti, come un alto numero di pacchetti SYN o RST. Questo può essere fatto tramite configurazioni del firewall o sistemi di prevenzione delle intrusioni (IPS).

Cattura di Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 - 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33842 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 - 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 - 896 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
92	36.778307838	192.168.200.100	192.168.200.150	TCP	74	54566 - 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	886 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 - 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 - 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	36.778614695	192.168.200.100	192.168.200.150	TCP	74	54282 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 - 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721688	192.168.200.150	192.168.200.100	TCP	60	286 - 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 - 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 - 54282 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 - 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.100	192.168.200.150	TCP	60	392 - 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.100	192.168.200.150	TCP	60	677 - 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	36.779029218	192.168.200.150	192.168.200.100	TCP	60	856 - 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 - 887 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145084	192.168.200.100	192.168.200.150	TCP	74	48138 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	897 - 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 - 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 - 196 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 - 48138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378639	192.168.200.100	192.168.200.150	TCP	74	50204 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397623	192.168.200.100	192.168.200.150	TCP	74	51262 - 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Analisi

Ancora una volta, possiamo notare un gran numero di pacchetti con flag RST/ACK e SYN.
Questa ripetizione conferma un attacco di SYN flood.

La quantità di pacchetti con lo stesso pattern di flag e simili indirizzi IP indica un comportamento anomalo e malevolo, tipico di tentativi di attacco che viene confermato anche dal fatto che non viene portato a termine il Three Way Handshake.

Oltre ai consigli dati sopra, si può anche pensare a segmentare la rete per poter isolare gli attacchi



L4 Traccia

Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

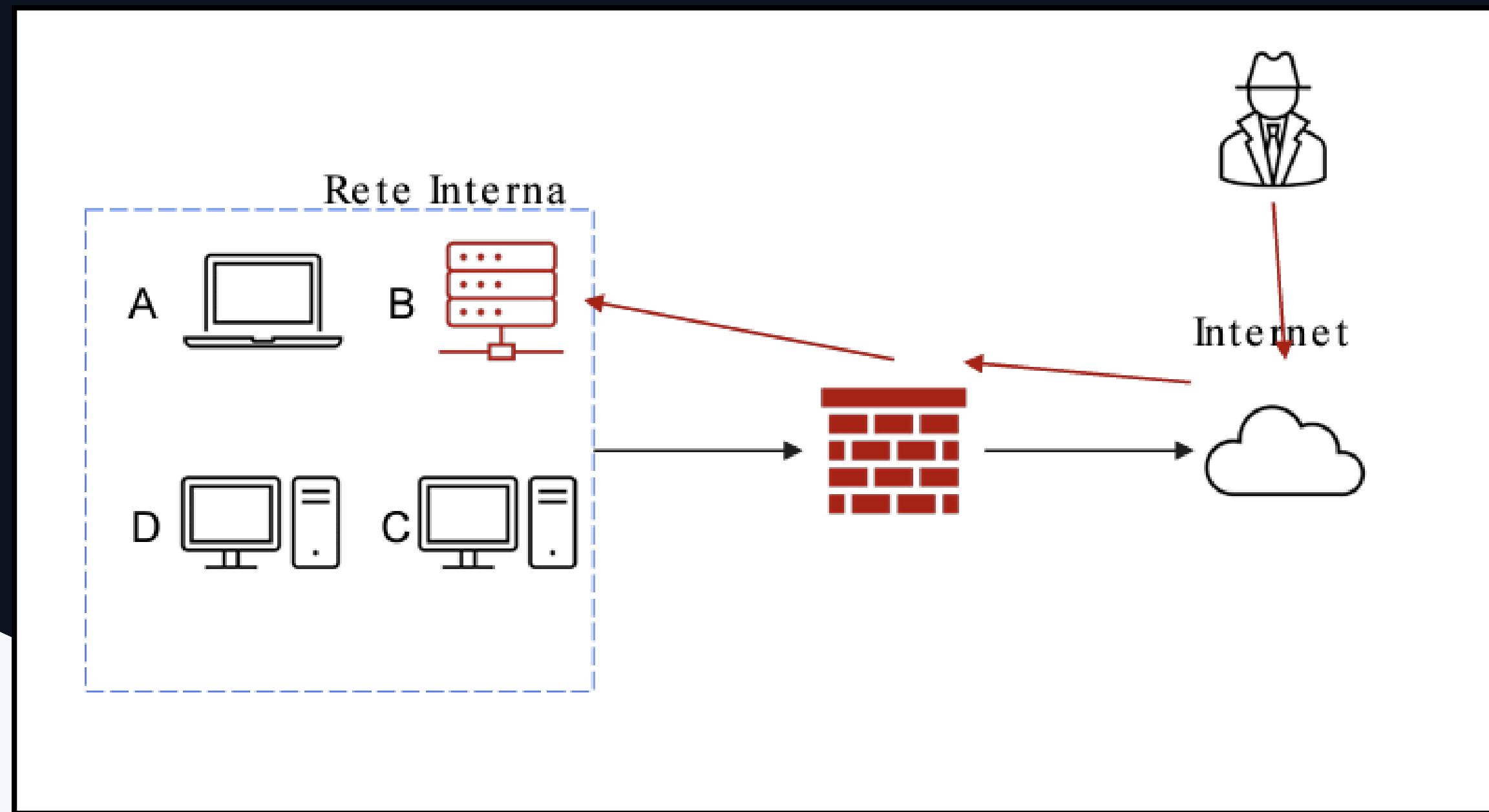
L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

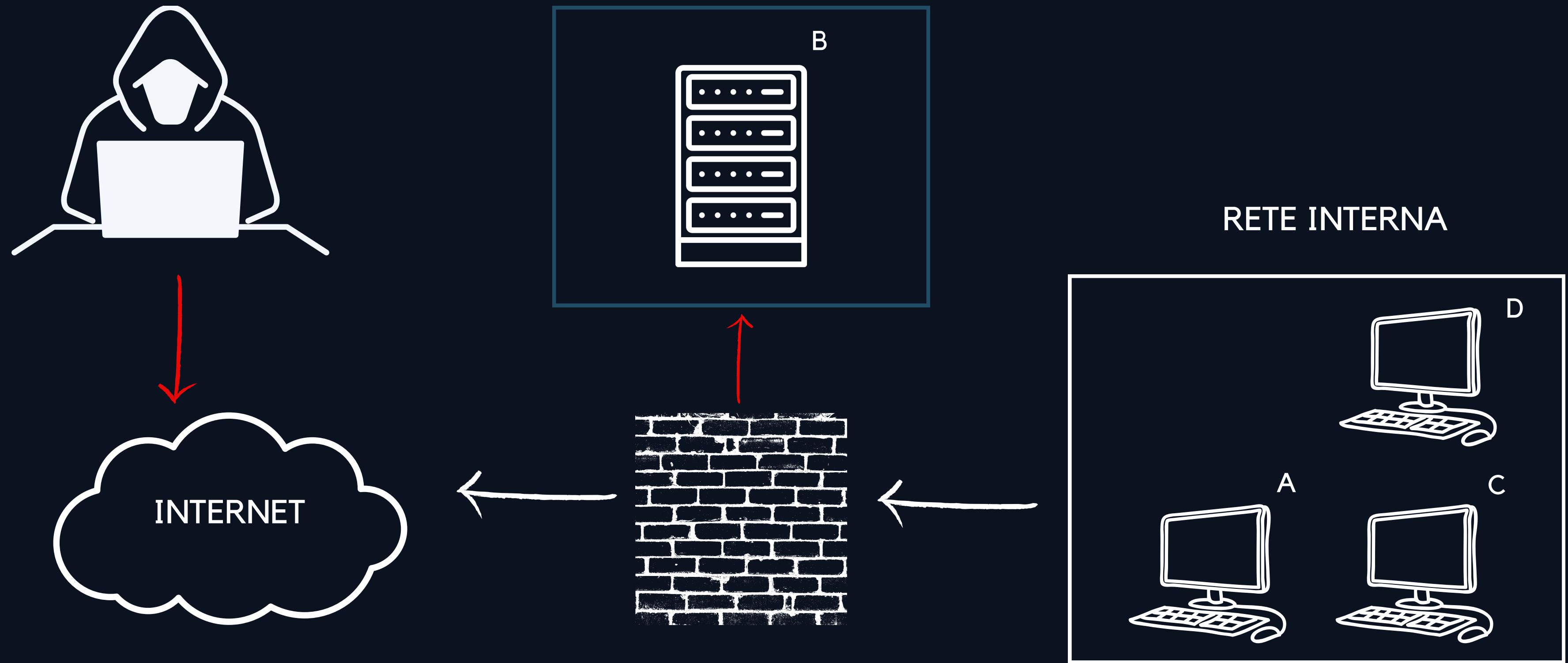
- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.

Indicare anche Clear

Immagine slide 4



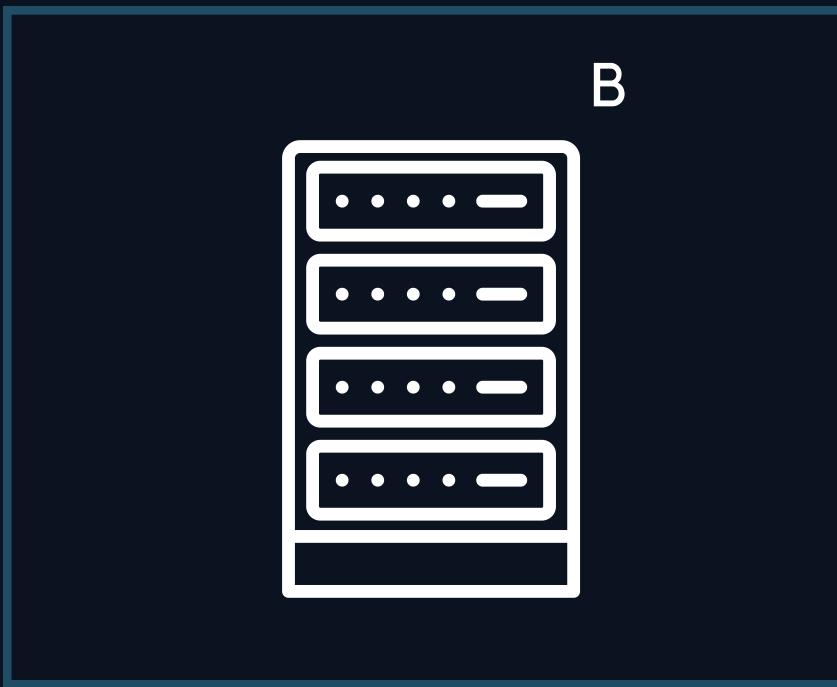
RETE DI QUARANTENA



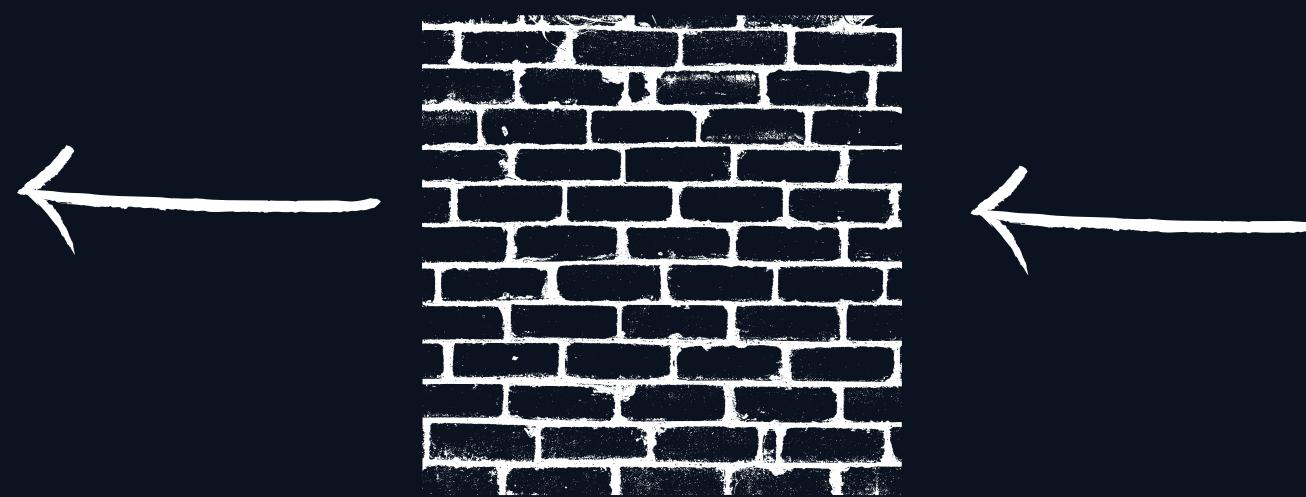
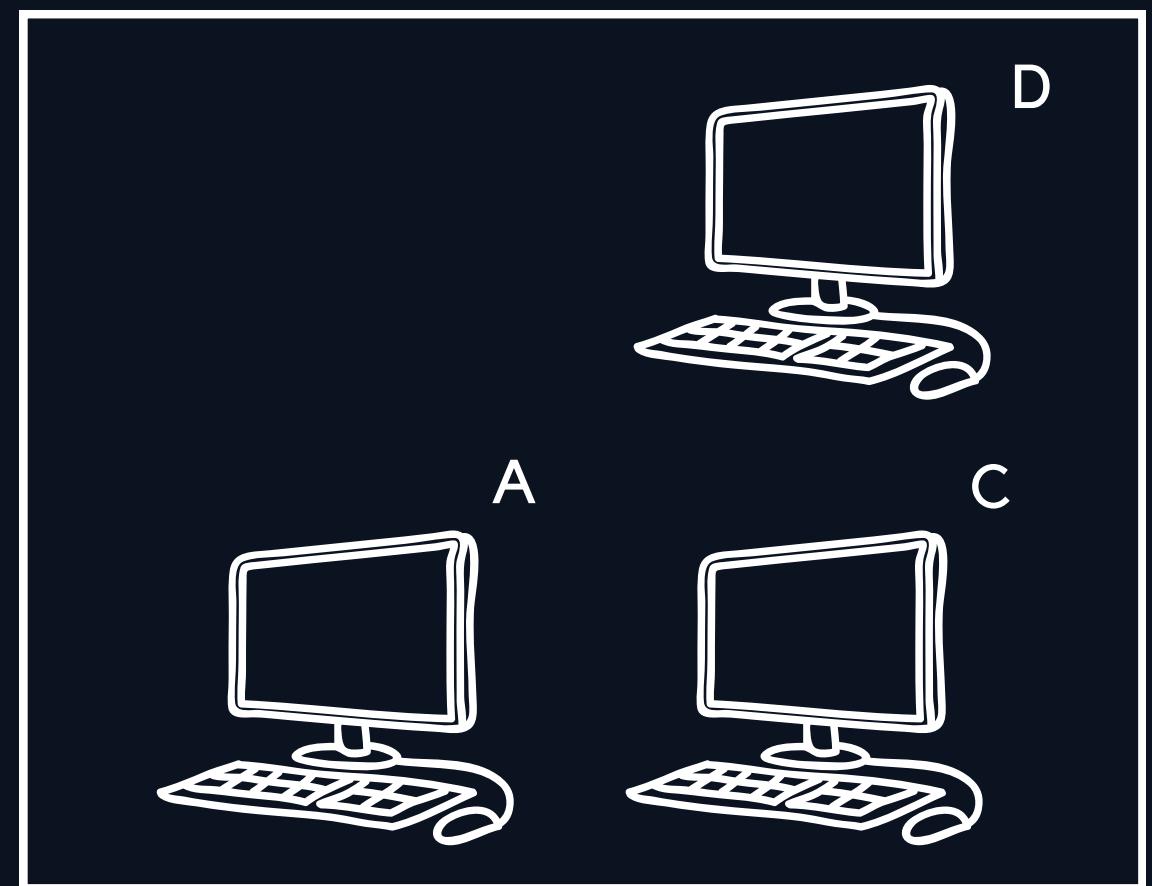
S9L1-5

ESEMPIO DI SOLAMENTO

RETE DI QUARANTENA



RETE INTERNA



INTERNET

S9L1-5

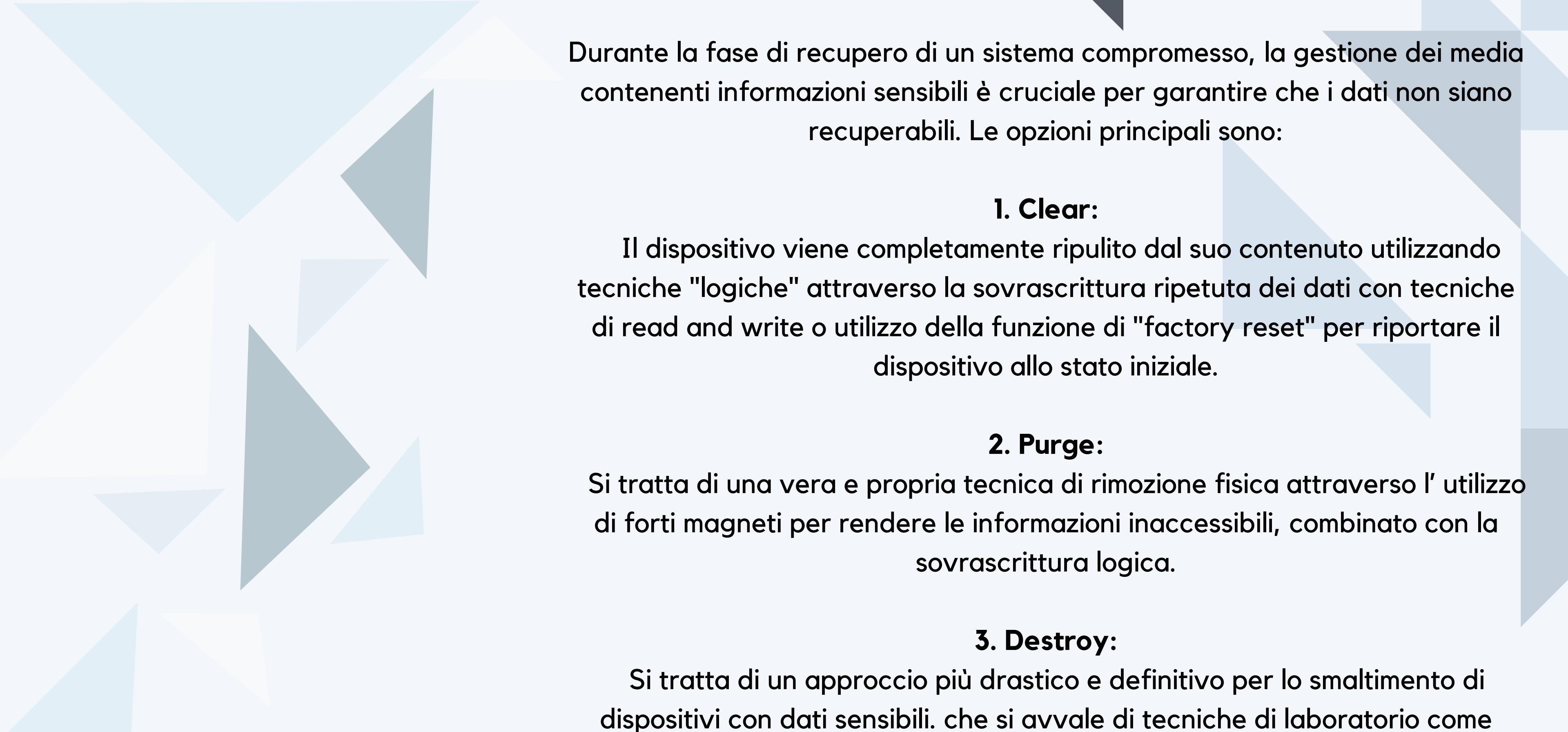
ESEMPIO DI RIMOZIONE

ISOLAMENTO

L'isolamento di un sistema infetto su una rete di quarantena implica scollegare il dispositivo infetto dalla rete principale e collegarlo a una rete separata per contenere la minaccia. L'attaccante in questo scenario ha comunque accesso al dispositivo infetto tramite internet. Questo processo prevede il rilevamento della minaccia, l'isolamento del dispositivo, l'analisi e la rimozione del malware, e il ripristino e reintegrazione del dispositivo nella rete principale solo quando è sicuro.

L'obiettivo è prevenire la diffusione della minaccia e proteggere l'integrità dell'intera rete.

A volte l'isolamento non basta a contenere la minaccia, e ci avvale quindi della tecnica di rimozione. Questa elimina completamente il sistema dalla rete, rendendolo inaccessibile sia da rete interna che da internet. Questo approccio fa sì che l'attaccante che non abbia più accesso nemmeno al sistema infetto. Anche in questo caso si passerà poi alla rimozione del malware e ripristino del dispositivo.



Durante la fase di recupero di un sistema compromesso, la gestione dei media contenenti informazioni sensibili è cruciale per garantire che i dati non siano recuperabili. Le opzioni principali sono:

1. Clear:

Il dispositivo viene completamente ripulito dal suo contenuto utilizzando tecniche "logiche" attraverso la sovrascrittura ripetuta dei dati con tecniche di read and write o utilizzo della funzione di "factory reset" per riportare il dispositivo allo stato iniziale.

2. Purge:

Si tratta di una vera e propria tecnica di rimozione fisica attraverso l' utilizzo di forti magneti per rendere le informazioni inaccessibili, combinato con la sovrascrittura logica.

3. Destroy:

Si tratta di un approccio più drastico e definitivo per lo smaltimento di dispositivi con dati sensibili. che si avvale di tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature e perforazione. Questi metodi garantiscono che le informazioni siano completamente inaccessibili, ma comportano un costo economico maggiore.

Quando un attacco è in corso su una rete interna e un sistema è compromesso, il team di CSIRT (Computer Security Incident Response Team) deve agire rapidamente per mitigare i danni e ripristinare la sicurezza della rete.

Contenimento

Nel caso dell' esempio riportato sopra, per prima cosa, è fondamentale contenere l'attacco immediatamente. Questo comporta l'isolamento del sistema B dalla rete per impedire all'attaccante di continuare ad accedere e diffondere la minaccia. Questo può essere fatto disconnettendo fisicamente il cavo di rete o modificando le regole del firewall per bloccare l'accesso. Inoltre, è importante proteggere i sistemi A, C e D, verificando se l'attacco si è esteso a questi dispositivi e isolandoli se necessario.

Analisi incidente.

Prima di eseguire qualsiasi azione di pulizia, è essenziale raccogliere tutte le prove possibili, come log di accesso, tracce di rete e snapshot del sistema, che saranno utili per l'analisi forense.

Identificare la vulnerabilità che ha permesso all'attaccante di compromettere il sistema B è cruciale; questo può includere l'analisi delle vulnerabilità di software, configurazioni errate o l'uso di credenziali compromesse.

Comunicazione e Contromisure

La comunicazione è un altro aspetto fondamentale. È necessario informare immediatamente tutti gli stakeholder rilevanti, inclusi gli amministratori di sistema, il management e il personale della sicurezza.

Per quanto riguarda le contromisure tecniche, è essenziale assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza e cambiare tutte le credenziali di accesso ai sistemi compromessi e a quelli potenzialmente affetti.

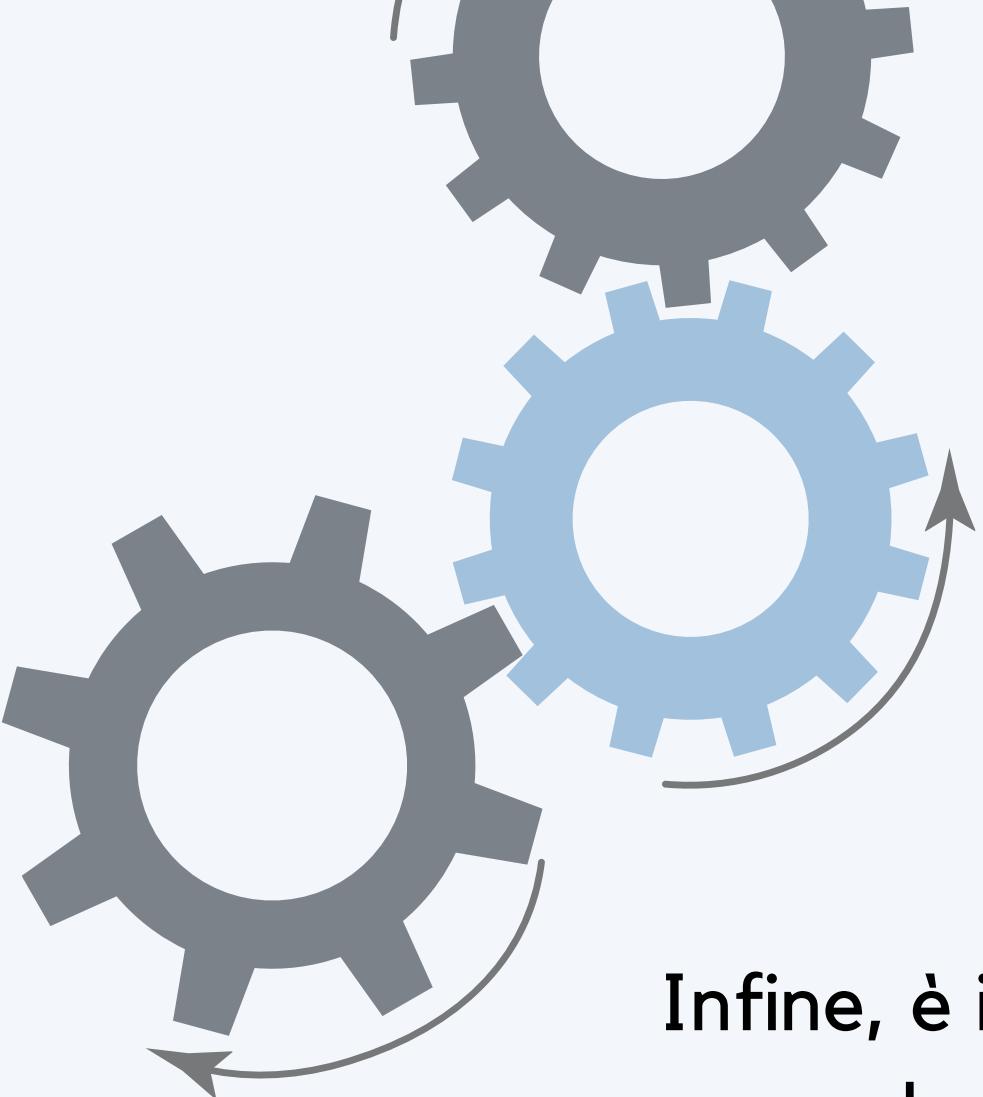
Rimozione

Una volta raccolte tutte le prove necessarie, si può procedere con la rimozione della minaccia. Questo implica una pulizia approfondita del sistema B, che potrebbe includere la reinstallazione del sistema operativo e del software applicativo. È anche necessario verificare l'integrità dei backup per assicurarsi che non siano stati compromessi e siano disponibili per il ripristino.

Ripristino

Il ripristino del sistema comporta la rimessa in sicurezza del sistema B e il ripristino dei dati dai backup sicuri.

Prima di rimettere il sistema in produzione, è essenziale eseguire test di penetrazione e verifiche di sicurezza per assicurarsi che il sistema sia sicuro.



Post-Incident

Infine, è importante eseguire una revisione dettagliata dell'incidente per comprendere cosa è successo, come è successo e cosa può essere migliorato.

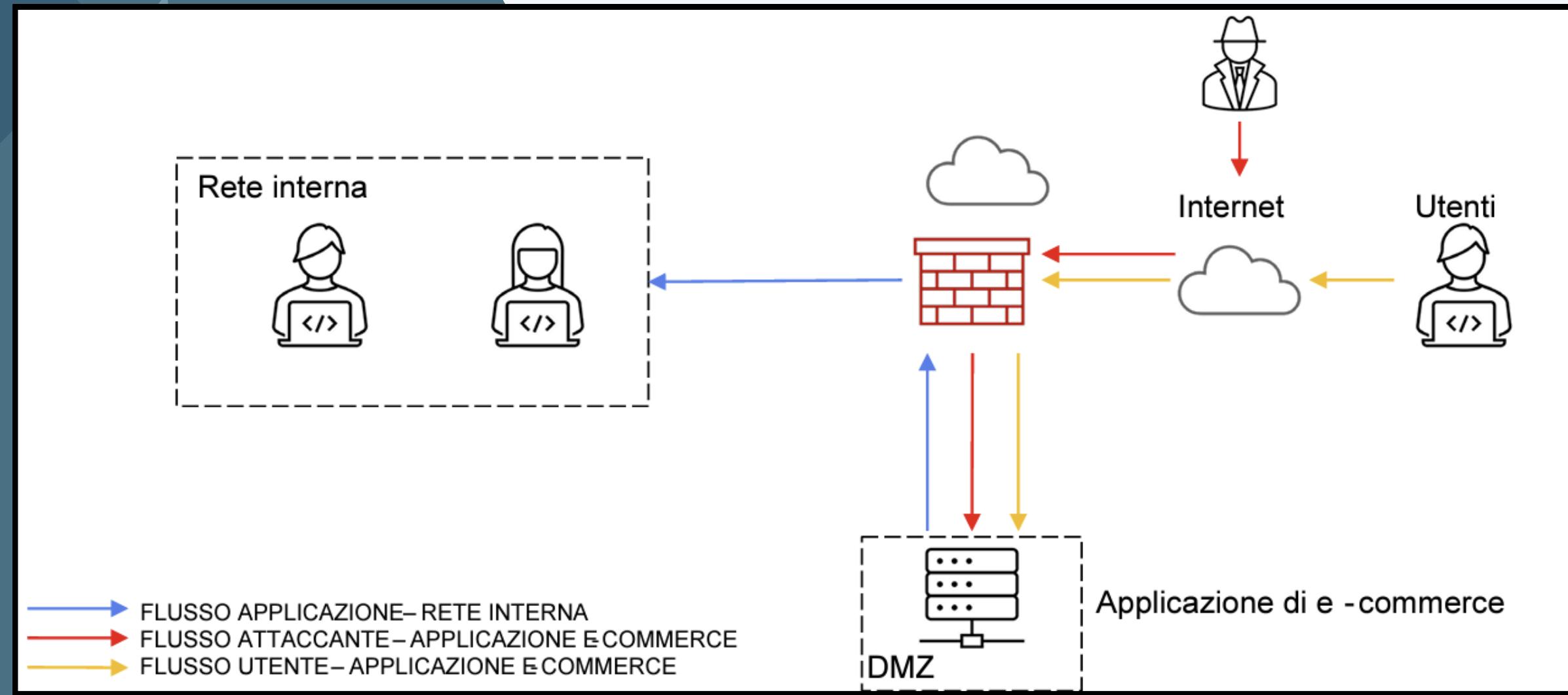
Aggiornare le procedure di sicurezza e di risposta agli incidenti in base alle lezioni apprese assicura che il team di CSIRT sia meglio preparato per affrontare futuri incidenti.



L5 Traccia

Con riferimento alla figura che segue, rispondere ai seguenti quesiti.

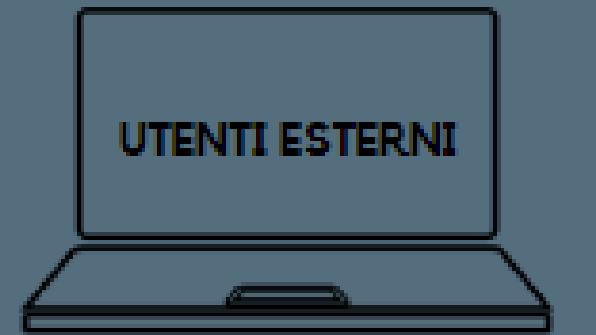
- 1. Azioni preventive** : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
- 2. Impatti sul business** : l'applicazione Web subisce 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 vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 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 necessario/facoltativo magari integrando la soluzione al punto 2)



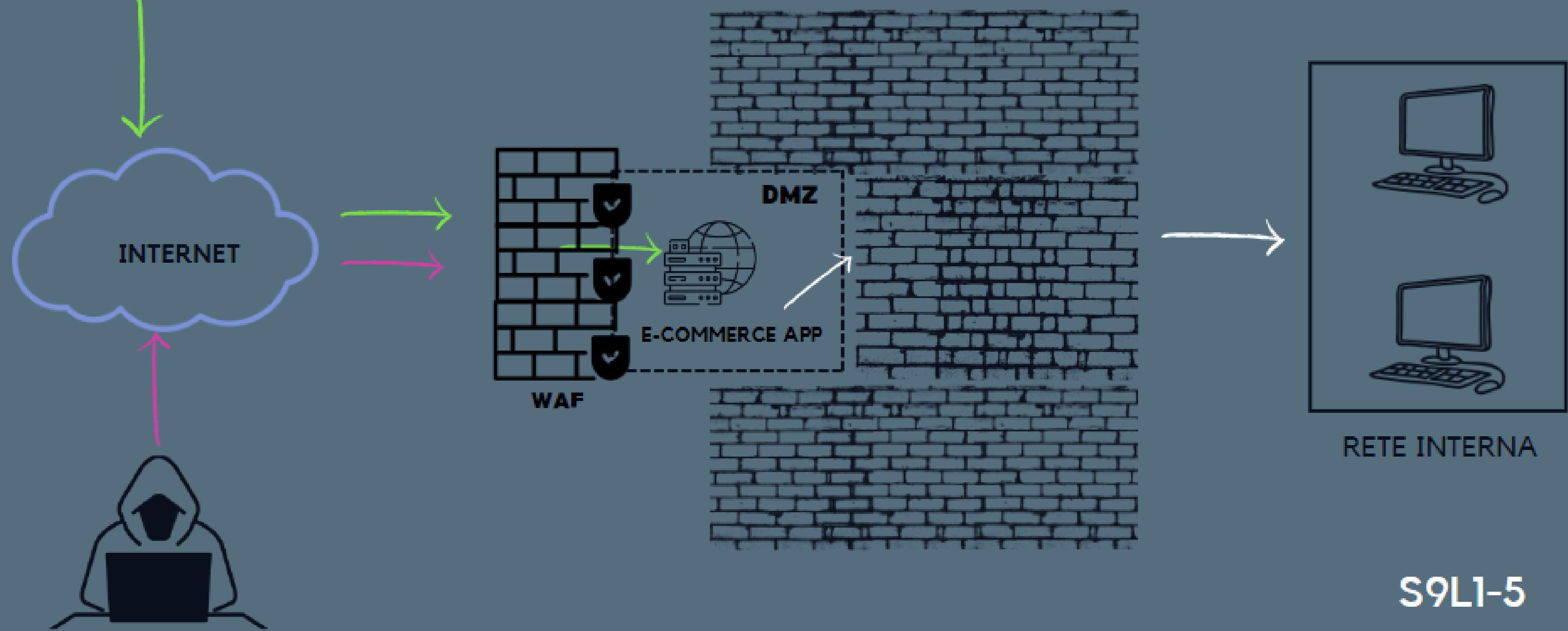
Architettura di rete:

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite 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.

AZIONI PREVENTIVE QUESITO 1



Per difendere l'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS) da parte di un utente malintenzionato, è consigliato configurare un Web Application Firewall (WAF) per monitorare e filtrare il traffico HTTP e HTTPS, bloccando richieste sospette.



QUESITO 2

Se l'applicazione web subisce un attacco DDoS che la rende non raggiungibile per 10 minuti, possiamo calcolare l'impatto economico basandoci sulla spesa media degli utenti.

- Spesa media degli utenti per minuto: 1.500 €
- Durata dell'attacco: 10 minuti

Calcolo:

Impatto sul business = Spesa media per minuto * Durata dell'attacco (in minuti)

$$\text{Impatto sul business} = 1.500\text{€} * 10\text{minuti} = 15.000\text{€}$$

Quindi, l'impatto economico dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000€.

AZIONI PREVENTIVE QUESITO 2

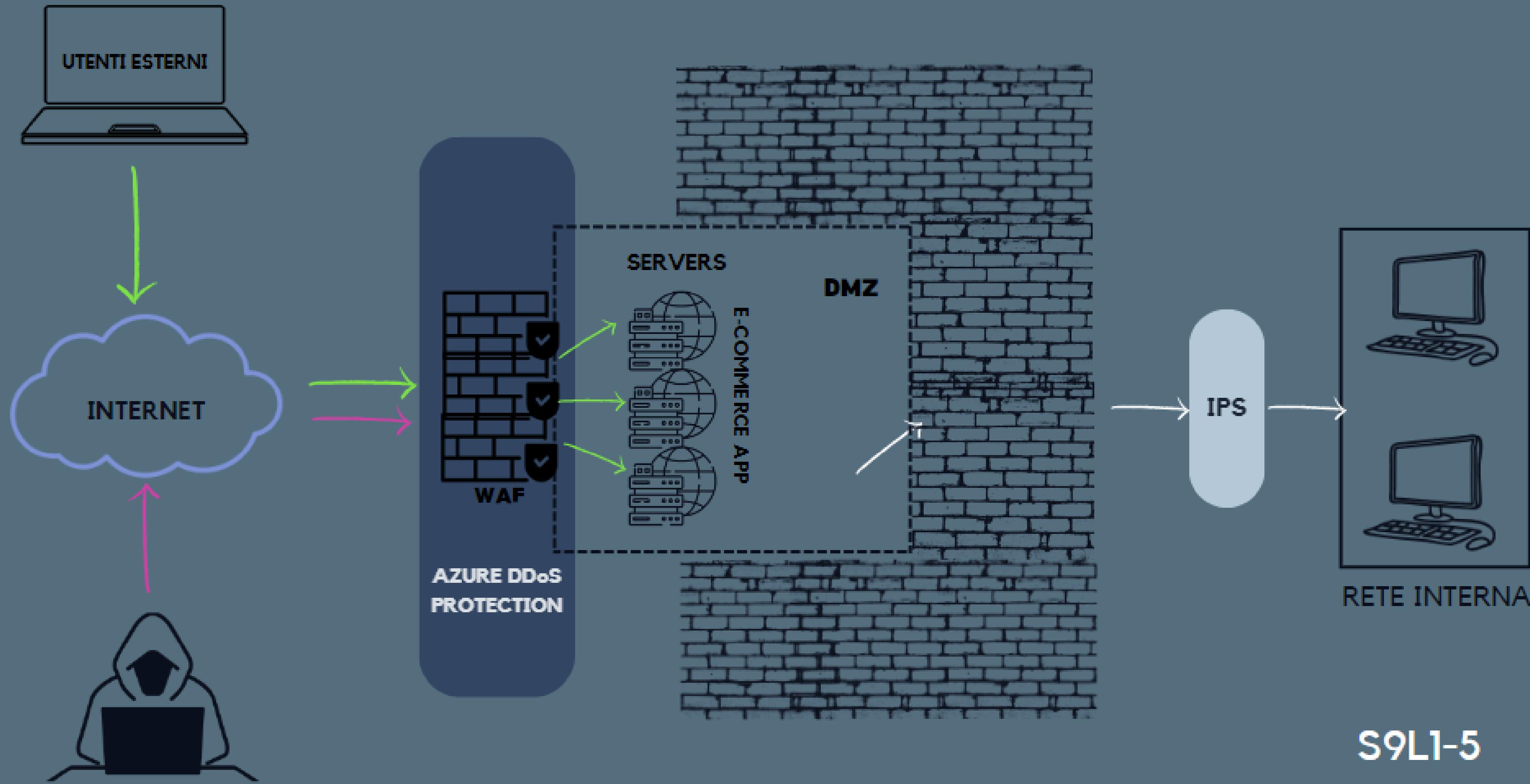
Per mitigare gli effetti di un attacco DDoS e ridurre l'impatto sul business, è possibile implementare le servizi che offrono protezione contro DDoS come Cloudflare o Azure DDoS Protection i quali possono rilevare e risolvere gli attacchi prima che raggiungano i server dell'applicazione.

Si può inoltre implementare un'architettura di rete ridondante con bilanciamento del carico (load balancing) per distribuire il traffico su più server. In caso di un attacco DDoS, il traffico viene distribuito su più risorse, riducendo l'impatto su singoli server.

Anche le tecniche di rate limiting sono una buona prevenzione in quanto limitano il numero di richieste che un singolo IP può fare in un dato periodo di tempo. Questo può aiutare a prevenire che un attaccante possa sovraccaricare il server con richieste eccessive tipico di un attacco DDos SYN flood.

Ovviamente l'utilizzo di firewall avanzati e sistemi IDS/IPS per rilevare e bloccare il traffico sospetto o malevolo insieme alle tecniche sopra, riducono drasticamente la riuscita di un attacco

ARCHITETTURA DI RETE CON AZIONI PREVENTIVE QUESITO 2



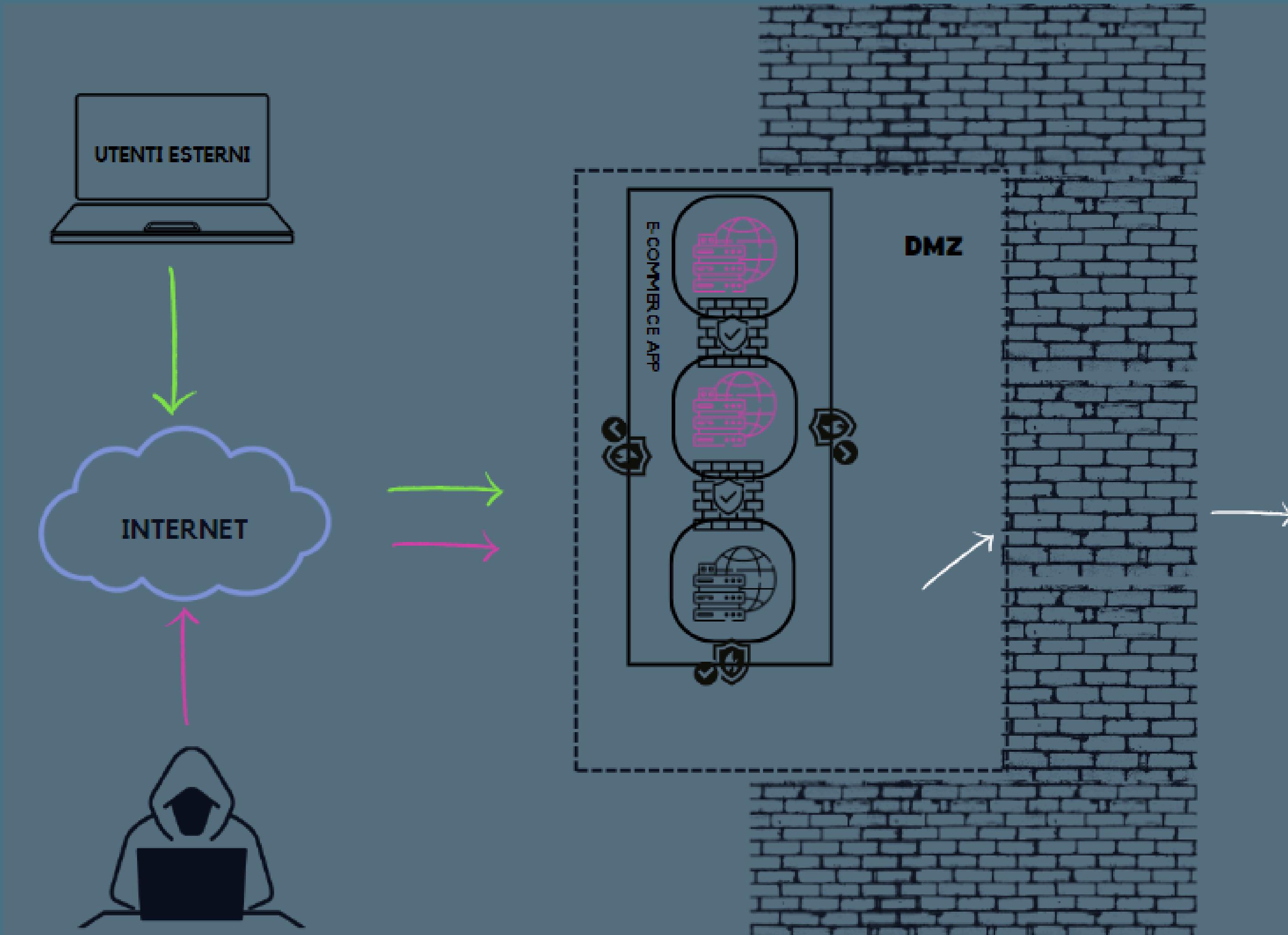
QUESITO 3

Per prevenire la propagazione del malware sulla rete, è essenziale implementare misure di contenimento che isolino il dispositivo infetto.

Nel disegno sotto ho provveduto a isolare i server della Web App creando delle zone di quarantena all' interno della DMZ.

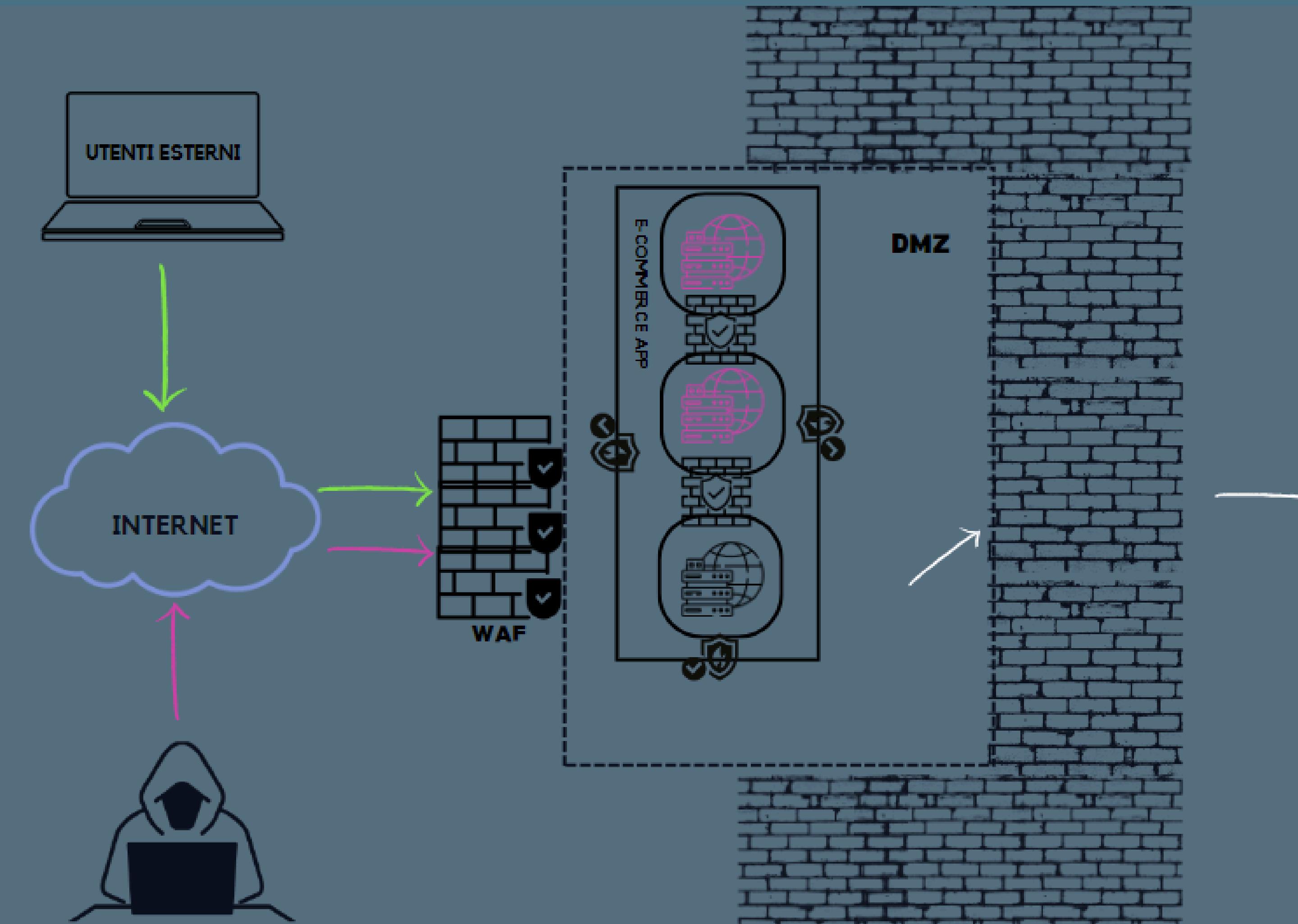
Siccome non sappiamo se tutti i server sono stati intaccati, ho deciso di assegnare ad ogni server una zona di quarantena diversa; così facendo, il server compromesso viene isolato in un segmento di quarantena, separato dagli altri server da firewall interni, il che previene la propagazione del malware agli altri server nella DMZ e alla rete interna.

RETE IMPLEMENTATA CON QUESITO 3



S9L1-5

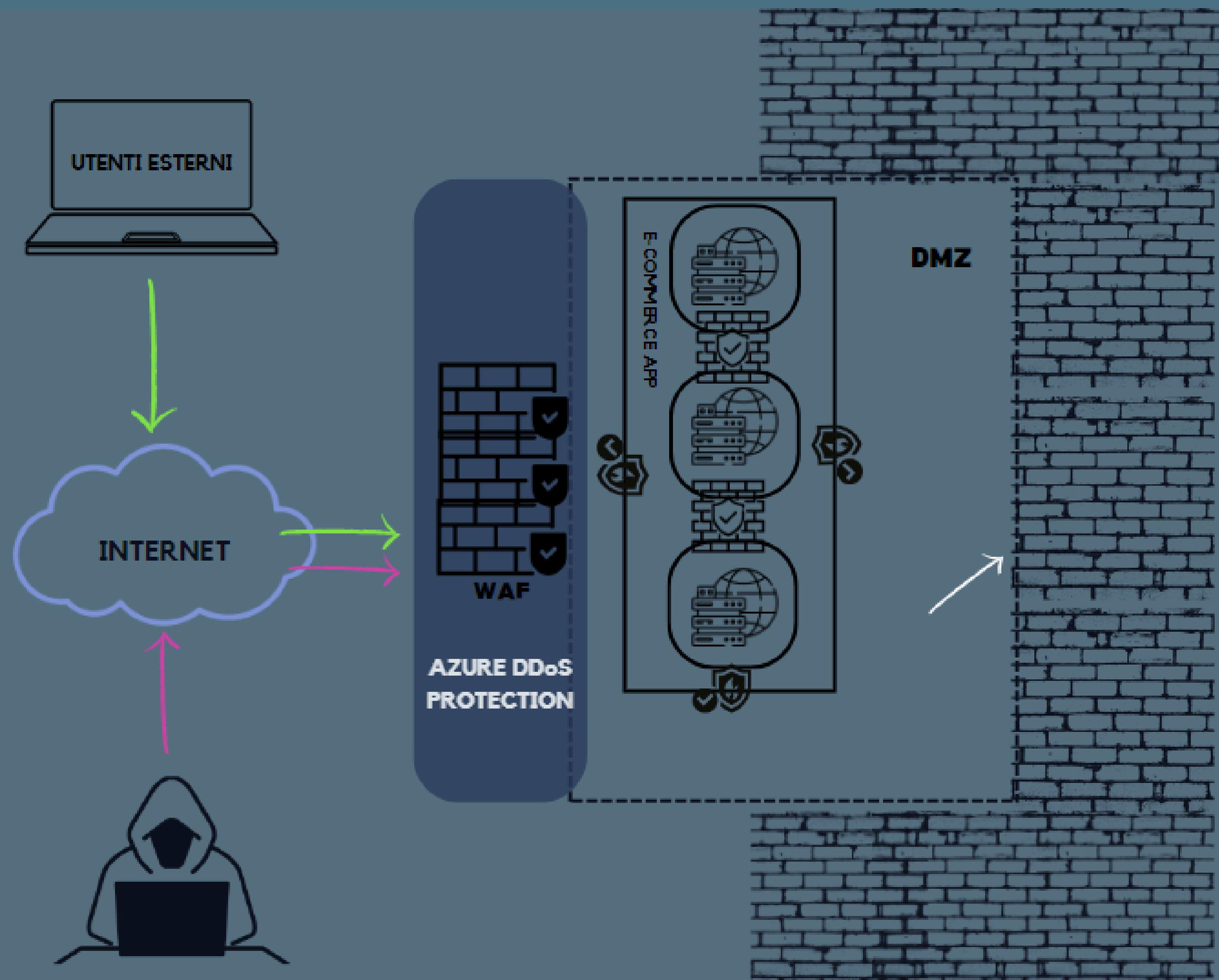
RETE IMPLEMENTATA UNENDO 1 e 3 (QUESITO 4)



RETE INTERNA

S9L1-5

INFRASTRUTTURA AGGRESSIVA QUESITO 5



S9L1-5

SPECIFICHE INFRASTRUTTURA AGGRESSIVA

- Nel disegno della rete, il WAF è stato posizionato per intercettare e filtrare traffico HTTP malevolo prima che raggiunga i server e-commerce.
- Azure DDoS Protection è stato invece implementato per prevenire attacchi DDoS e garantire la continuità del servizio.
- L'IPS monitora e previene intrusioni verso la rete interna, bloccando il traffico sospetto.
- I server nella DMZ sono stati isolati in segmenti separati tramite firewall interni per prevenire la propagazione del malware in caso di infezione; infatti, in caso succedesse, il server compromesso verrebbe isolato in un segmento di quarantena, mantenendo al sicuro gli altri server e la rete interna. I firewall interni sono stati posizionati tra i segmenti della DMZ per applicare politiche di sicurezza rigorose e isolare i server infetti.
- Un sistema di monitoraggio e logging raccoglie dati in tempo reale, permettendo una risposta rapida alle minacce.

Conclusioni

L'implementazione delle misure di sicurezza descritte offre una protezione robusta per l'applicazione di e-commerce, garantendo la sicurezza delle informazioni trattate e la continuità del servizio. Il WAF, la protezione DDoS e l'IPS lavorano in sinergia per prevenire e mitigare attacchi esterni, mentre l'isolamento dei server infetti e i firewall interni assicurano che eventuali compromissioni non si propaghino all'interno della rete. Il monitoraggio continuo permette di mantenere un elevato livello di sicurezza, rilevando e rispondendo rapidamente a qualsiasi minaccia. L'architettura risulta quindi ben protetta contro una vasta gamma di minacce, garantendo allo stesso tempo la disponibilità e l'integrità del servizio e-commerce.