PROGETTO U359L5

VITTORIO BRACCIA - NETREBELS

TRACCIA

Con riferimento alla figura nella 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. È richiesta sola modifica

2. **Impatti sul business** : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

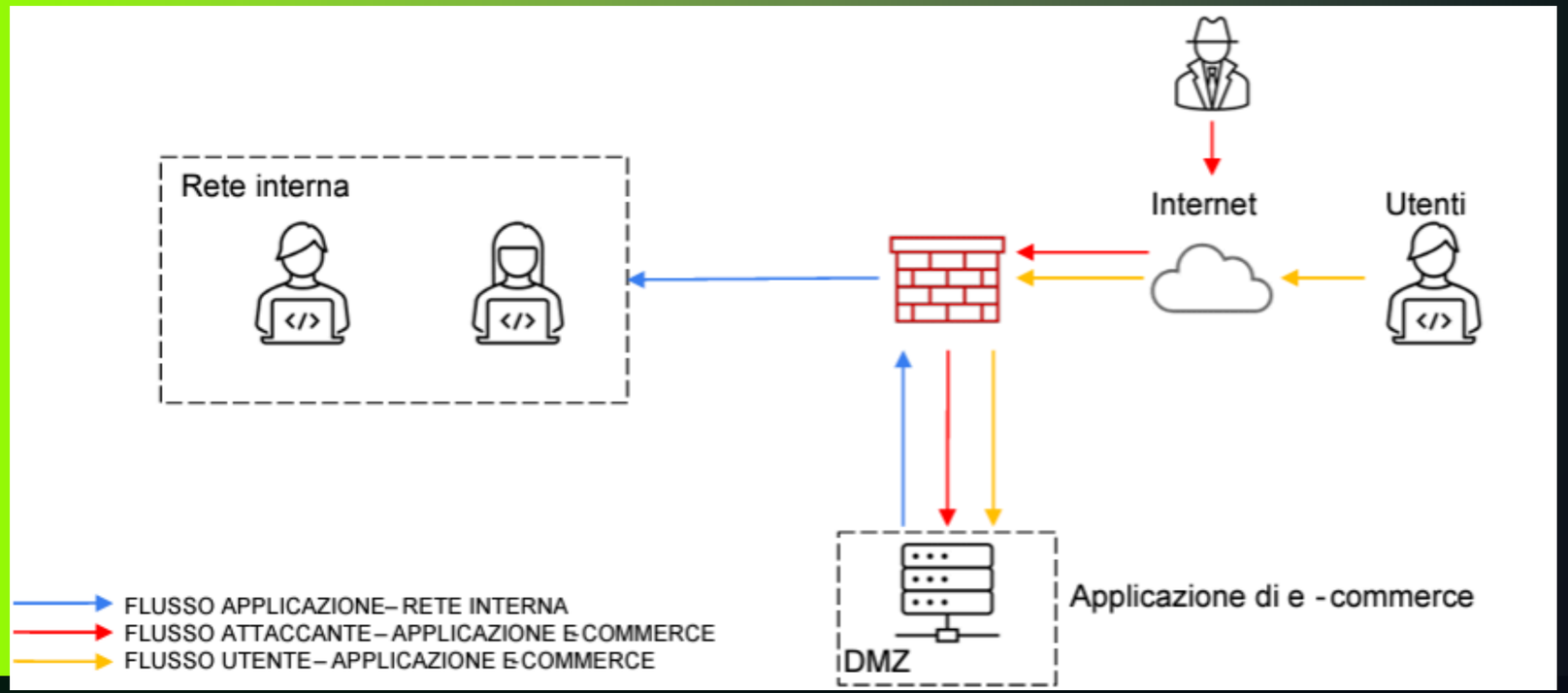
3. **Response** : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta

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 (integrando anche una soluzione al punto 2)
Budget 5000 - 10000 euro. Eventualmente fare più proposte di spesa

TRACCIA

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.

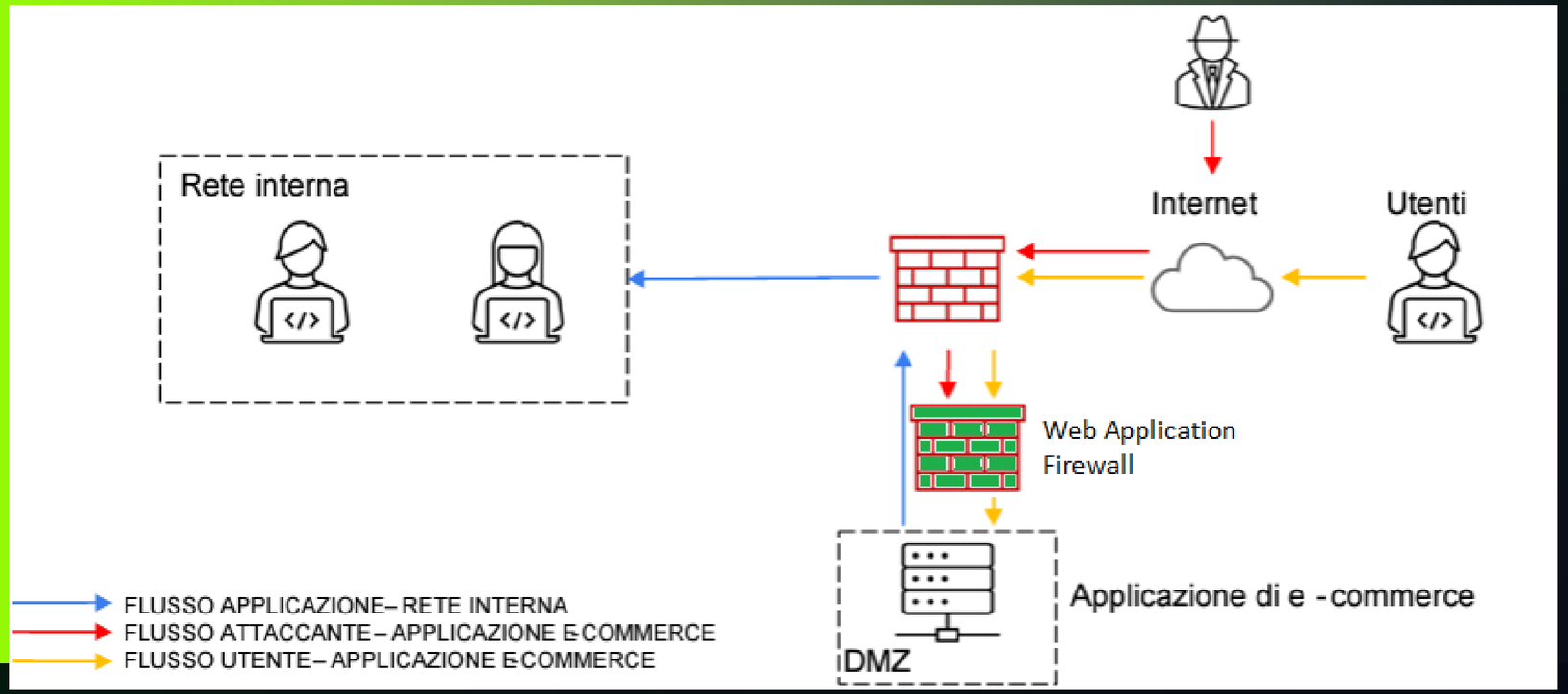


RISOLUZIONE

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. È richiesta sola modifica

Per proteggere la Web App da minacce come XSS e SQLi, è possibile adottare un Web Application Firewall (WAF). A differenza dei firewall tradizionali, i WAF sono specificamente progettati per difendere le applicazioni web da questi tipi di attacchi . Un WAF può filtrare e monitorare il traffico HTTP verso e dalla tua applicazione web, bloccando attacchi noti come ,appunto, XSS e SQLi. Molti WAF includono regole predefinite per riconoscere e prevenire questi tipi di attacchi.



RISOLUZIONE

2

Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Sapendo che questo attacco DDoS blocca l'applicazione Web per 10 min e che gli utenti spendono circa 1.200 € ogni minuto. Si può facilmente calcolare l'impatto che questo attacco ha sul buisness moltiplicando i minuti di irraggiungibilità del servizio per la media del soldi spesi al minuto dagli utenti.

Impatto sul business = 10 x 1200 = 12000 €

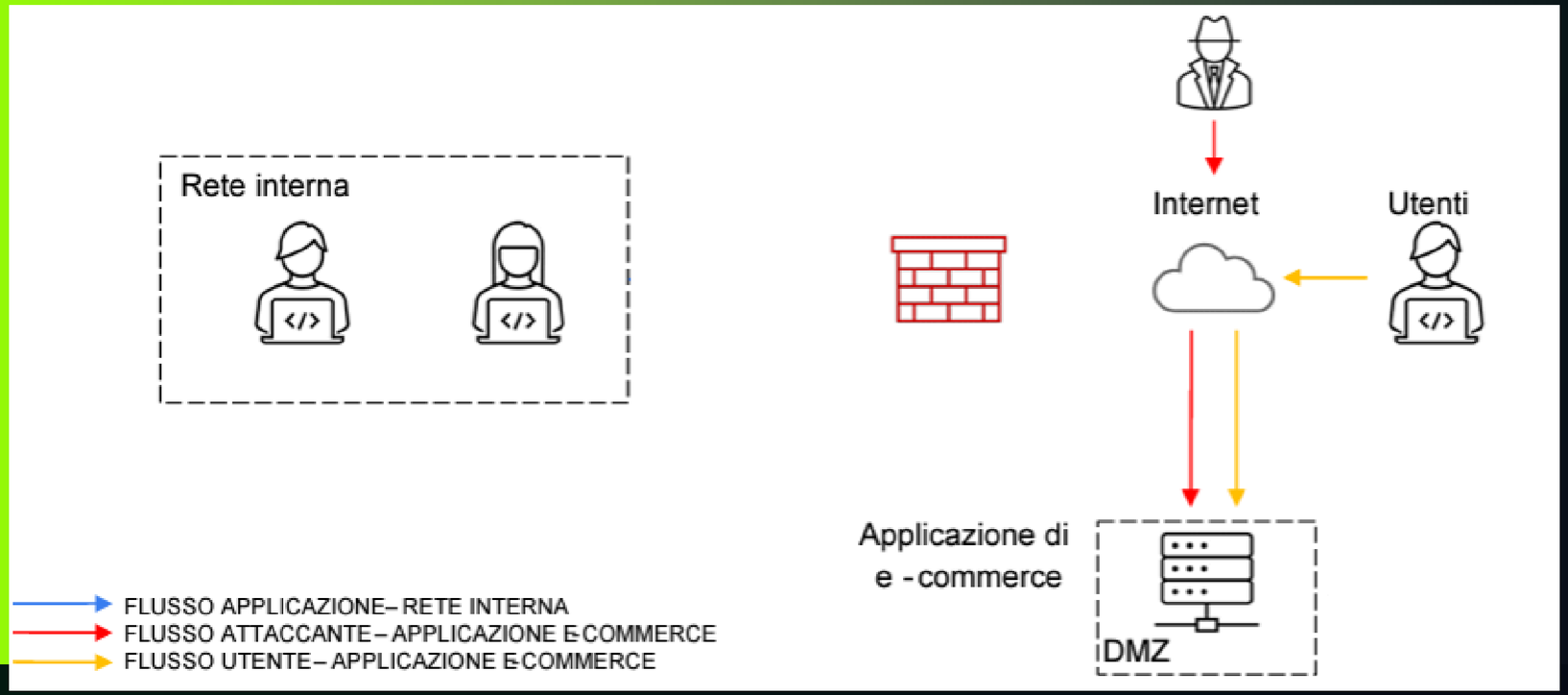
In pratica questo attacco a fatto perdere all'azienda un possibile guadagno di 12.000 €

RISOLUZIONE

3

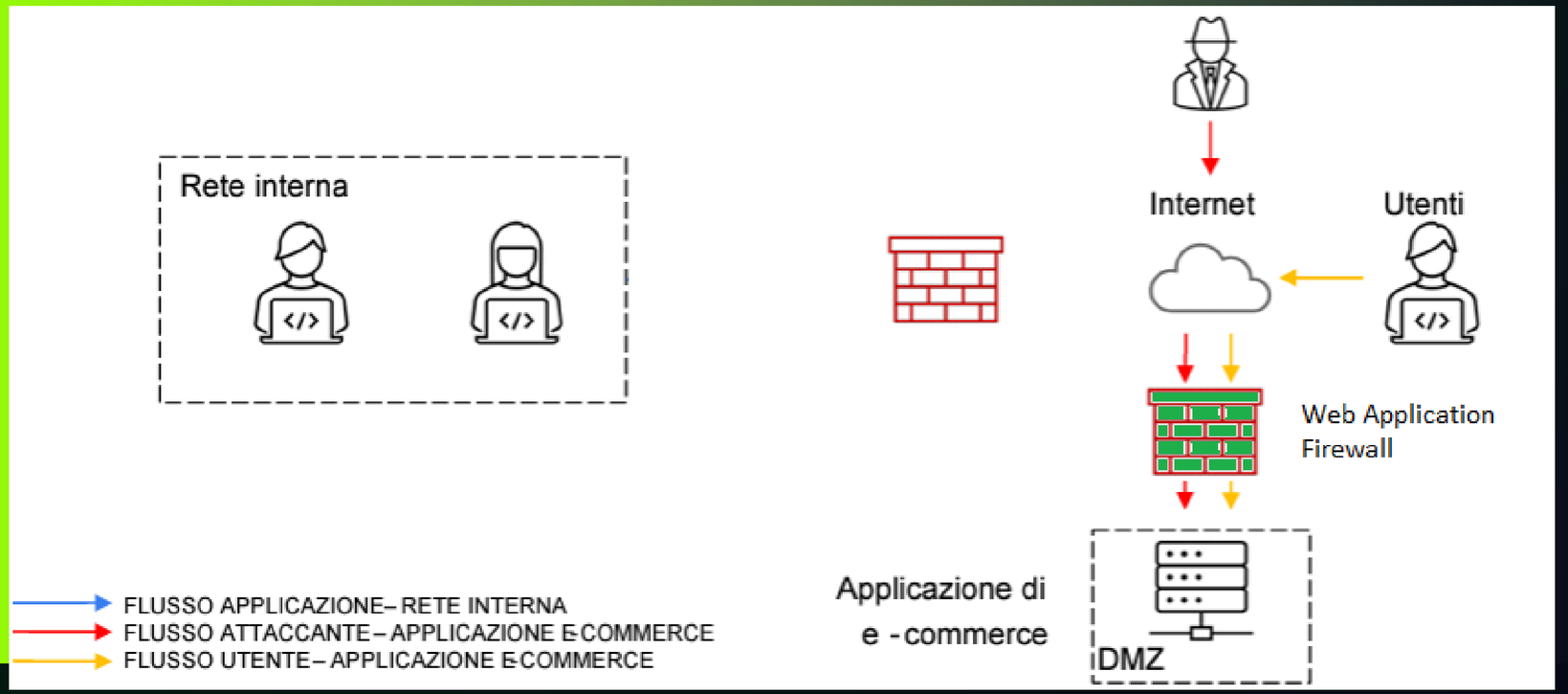
Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 3 con la soluzione proposta

Visto che dobbiamo evitare che il malware si propaghi, la soluzione migliore sarebbe quella di isolare l'applicazione web infetta. Staccheremo l'applicazione dalla rete interna ma la lasceremo attaccata ad internet, così che rimanga raggiungibile da chi ci sta attaccando



RISOLUZIONE

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



RISOLUZIONE

5

Modifica «più aggressiva» dell’infrastruttura: integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2)
Budget 5000 - 10000 euro. Eventualmente fare più proposte di spesa

Ecco una possibile proposta per un eventuale modifica all’infrastruttura

Next geration Firewall. Un nuovo firewall dedicato per una protezione aggiuntiva.
Costo Stimato: 1.500-3.000 euro.

Sistema di Prevenzione delle Intrusioni (IPS) e Rilevazione delle Intrusioni (IDS)
Una combinazione di IPS e IDS per monitorare e prevenire attività sospette.
Costo Stimato: 1.500-2.500 euro.

Servizio di Mitigazione DDoS: Utilizza un servizio di mitigazione DDoS basato su cloud.
Costo Stimato: 1.000-2.000 euro all'anno.

WAF: Protezione delle applicazioni web contro attacchi come XSS e SQLi.
Costo Stimato: 1.000-2.000 euro.

Backup: Soluzioni di backup regolari e sicure.
Costo Stimato: 600-1.200 euro.

Costo Minimo 5600 euro
Costo Massimo 10700 euro

BONUS

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

1 https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /

2 https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2 /

BONUS

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

1

https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /

Dal link possiamo notare:

Il PDF tenta di connettersi a un sito esterno è sospetto, soprattutto se il sito non è conosciuto o fidato.
Questo è tipico delle email di phishing che utilizzano allegati PDF con link malevoli per indurre l'utente a scaricare ulteriori malware o inserire informazioni sensibili.

Il programma, AnyRun, ha rilevato attività sospetta e potenzialmente malevola legata all'apertura del file PDF.
Le richieste HTTP fallite indicano che il malware ha tentato di comunicare con server esterni, probabilmente per scaricare ulteriori payload.

Questo tipo di attacco sembra proprio un attacco di spear phishing. E’ un tipo di attacco di phishing che prende di mira uno specifico individuo o gruppo di individui all'interno di un'organizzazione e tenta di indurli con l'inganno a divulgare informazioni sensibili, a scaricare malware o a inviare o autorizzare involontariamente pagamenti all'aggressore

BONUS

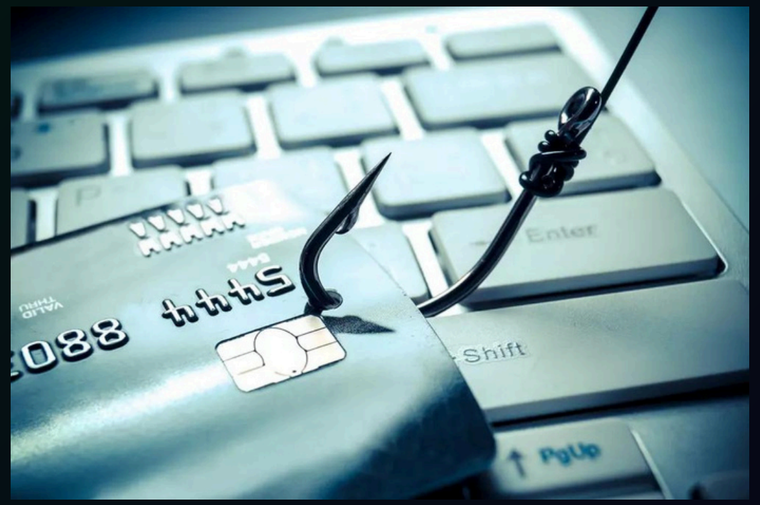
Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo all'eventuale attacco spiegando ad utenti e manager la tipologia di attacco e come evitare questi attacchi in futuro:

1

https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /

Ecco alcune operazioni per evitare questi attacchi di phishing:

- Controllare attentamente l'indirizzo email del mittente
- Non cliccare su link sospetti
- Non aprire allegati provenienti da mittenti sconosciuti o sospetti
- Riconosci i segnali di phishing, come messaggi urgenti, richieste di informazioni personali



BONUS

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

2

https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2 /

Dal link fornito , è chiaro che il sistema è stato infettato da un ransomware della famiglia Phobos, che include anche capacità di furto di informazioni (stealer):

Sulla destra, Any.Run mostra un'indicazione di attività malevola ("Malicious activity") con vari processi e connessioni di rete. Il malware è identificato con un hash MD5 specifico e classificato come ransomware/stealer della famiglia Phobos,in oltre, viene indicata l'attività di diversi processi sospetti e malevoli.

BONUS

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

2

https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2 /

Alcune prevenzioni e possibili riposte ad un attacco Ransomware:

Prevenzione:

- Backup Regolari: Effettuare regolarmente backup dei dati critici e conservare una copia offline
- Aggiornamenti: Mantenere tutti i software e sistemi operativi aggiornati con le ultime patch di sicurezza

Risposte:

- Isolamento: Isolare immediatamente i dispositivi infetti dalla rete per prevenire la diffusione del ransomware
- Recupero dei Dati: Utilizzare i backup non infetti per ripristinare i dati