# ESERCIZIO W14D4

L’esercizio di oggi ci porta a fare brainstorming su un caso di wannacry. La traccia da seguire riporta tali indicazioni:

- Hai appena scoperto che l’azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry.
- Cosa fai per mettere in sicurezza il tuo sistema?

## Fase 1: Scollegamento end point infetto

Per cominciare, la prima task riguarda proprio scollegare dalle reti WAN e LAN il Windows 7 infettato dal ransomware. In questo modo fermo il ransomware dal mietere altri bersagli.

## Fase 2: Scollegamento dispositivi di rete

Successivamente, vado a scollegare le tecnologie di rete: WI-FI, Switch, Router etc. Non posso essere sicuro, almeno non subito, di quanto il danno sia esteso all’interno della LAN. Cosi lavoro anche con più calma.

## Fase 3: Ulteriore controllo dei computer aziendali

Mi assicuro che il computer con Windows 7 sia l’unico ad essere stato colpito da Wannacry. Quando ho certezza dei numeri, procedo con il resettare le credenziali dei vari dispositivi, per impedire altre compromissioni.

## Fase 4: Cancellare i sistemi infetti e reinstallare l'OS

Una volta messi in sicurezza i bersagli colpiti, elimino completamente il loro sistemi e reinstallo gli OS a partire dai backup precedenti ai suddetti. Verifico inoltre che i backup utilizzati siano liberi dal ransomware.

Pro: Ripristinare o reinstallare il sistema operativo può rimuovere il malware dai file di sistema.

Contro: Possibile perdita di dati se i backup non sono disponibili o riparati dalla rete aziendale.

## Fase 5: Aggiornamento sistemi

Come prossimo passo, confido che aggiornare il sistema possa correggere le falle nella sicurezza che hanno permesso in primis al ransomware di attecchire.

Pro: L'aggiornamento garantisce che tutte le vulnerabilità note siano corrette, riducendo il rischio.

Contro: Potrebbe non essere sufficienti a garantire la sicurezza, nel caso di una nuova versione del ransomware che sorpassa persino gli aggiornamenti passati di Windows sui suoi sistemi end of life.

## Fase 6: Utilizzo strumenti anti-malware

Per essere sicuro della completa pulizia del sistema, o di essermel giocate tutte, effettuo una diagnostica con un software anti-malware avente funzionalità anti-ransomware.

Pro: Possono aiutare a individuare e rimuovere il malware esistente ed i suoi servizi in modo efficace.

Contro: Potrebbero non sempre riuscire a eradicare completamente i malware sofisticati.

## Fase 7: Riattivazione rete e altri controlli

Ricollego la rete aziendale ai suoi end-point ed effettuo ulteriori controlli sia con l’antivirus che a livello di network traffic.