TIPO: ATTACCO INFORMATICO OBIETTIVO: TUTTI	ATTACCO RANSOMWARE - indisponibilità massiccia di postazioni di lavoro	

1. Allerta

Rapporto sull'attacco (messaggio sul desktop, file e applicazioni inaccessibili...)	Segnalazione al SOC
NON CANCELLARE NULLA : tutte le informazioni verranno utilizzate come prove nelle indagini	**PRENDERE SUBITO ATTO DELLA SEGNALAZIONE**
NON APRIRE FILE O APPLICAZIONI CRIPTATE: bisogna bloccare l'infezione	**CONDIVIDERE TUTTE LE INFORMAZIONI** con il SOC per valutare la portata dell'attacco e le priorità di risposta all'emergenza
	SEGUIRE LE ISTRUZIONI DEL COS

2. Azioni d'emergenza

1. **Isolamento dei sistemi essenziali :**
   - Scollegare tutte le reti
   - Scollegare il cavo di rete dai computer
   - Scollegamento delle connessioni WiFi
2. Scollegare tutti i dispositivi
3. Se non si riesce a disconnettere il computer dalla rete, **disattivare tutti i router e gli hotspot Wi-Fi**
4. Valutare la portata della violazione **e raccogliere prove**

3. Soluzione di continuità

Fornitura di un ambiente di lavoro virtualizzato accessibile da Internet tramite qualsiasi postazione di lavoro, in ordine di criticità delle attività.

4. Criteri per l'attivazione della soluzione di continuità

È l'unità di crisi che prende la decisione finale di attivare il PCA.

Criterio 1: il 5% delle postazioni di lavoro è inutilizzabile

Criterio 2: rischio di propagazione del ransomware ad altri siti / entità / applicazioni