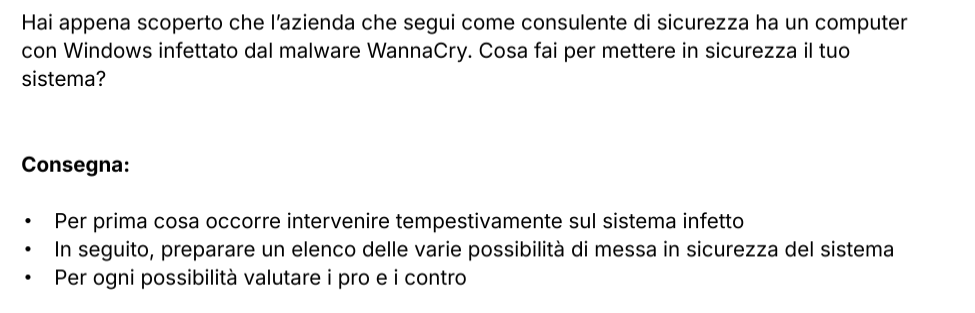
**W14D1(facoltativo) TULLI ROBERTO**

**PASSWORD CRACKING E MALWARE**

Roma 08/10/2025

**Traccia:**

****

**Azioni immediate:**

**1. Isolare il computer infetto** – Scollegarlo immediatamente dalla rete (staccare cavo ethernet o disabilitare WI-FI) per evitare che il ransomware si propaghi ad altri PC.

**2. Non spegnere il computer** – Lasciarlo acceso per preservare dati in RAM utili per analisi forensi e per recuperare i dati.

**3. Documentare** lo stato del sistema (screenshot, log, processi attivi)

**4. Avvisare immediatamente l’azienda** e tutti gli utenti della rete.

**5. Identificare** quali file sono stati criptati e se esistono backup recenti

**Azioni successive:**

**1. Ripristino da backup** (soluzione ideale se disponibile)

* Verificare esistenza di backup recenti e integri
* Ripristinare il sistema da backup pulito

**2. Utilizzo di decryptor** (se disponibile)

* Verificare se esistono tool di decryption per la variante specifica

**3. Ripristino completo**

* Formattazione e reinstallazione pulita del sistema
* Reinstallazione applicazioni da fonti sicure

**4. NON pagare il riscatto (fortemente sconsigliato)**

* Non garantisce recupero dati
* Finanzia attività criminali

**5. Controllare se altri PC sono infetti**

### **Valutazione Pro e Contro**

**RIPRISTINO DA BACKUP**

* **✅ Pro:** Recupero completo dei dati, sistema pulito, nessun rischio residuo
* **❌ Contro:** Possibile perdita di dati recenti (dal ultimo backup), richiede tempo

**UTILIZZO DECRYPTOR**

* **✅ Pro:** Potenziale recupero dati senza perdite, più veloce
* **❌ Contro:** Non sempre disponibile o efficace

**RIPRISTINO COMPLETO**

* **✅ Pro:** Sistema garantito pulito, elimina tutte le minacce
* **❌ Contro:** Perdita totale dei dati se non c'è backup

**PAGAMENTO RISCATTO**

* **✅ Pro:** Teoricamente recupero immediato (ma NON garantito)
* **❌ Contro:** Finanzia criminali, nessuna garanzia, possibili riattacchi, sistema compromesso rimane vulnerabile

## **Azioni Aggiuntive Fondamentali**

### Per l'intero sistema aziendale:

1. **Scansione completa di tutti i sistemi della rete**
2. **Verifica e aggiornamento delle politiche di backup**
3. **Segmentazione della rete per limitare propagazione futura**
4. **Formazione del personale su phishing e sicurezza**
5. **Piano di Risposta agli Incidenti (documento che definisce ruoli e procedure per gestire emergenze di sicurezza)**

**Raccomandazione finale: Isolare il sistema infetto, ripristinare da backup, Installare l'aggiornamento MS17-010 che protegge dalla vulnerabilità sfruttata da WannaCry e implementare controlli preventivi per evitare futuri incidenti.**