

W14D1

Se scopri che un computer con Windows 7 in un'azienda che segui come consulente di sicurezza è stato infettato dal malware WannaCry, è cruciale agire immediatamente per contenere la minaccia e minimizzare i danni. Ecco un piano dettagliato per mettere in sicurezza il sistema:

1. Misure reattive:

1. Isolamento del sistema infetto

- **Pro:**
 - Impedisce la diffusione del malware ad altri sistemi della rete.
 - Facilita l'analisi e la pulizia del sistema infetto.
- **Contro:**
 - Il sistema infetto potrebbe rimanere inutilizzabile durante l'isolamento.
 - Non risolve il problema immediato dei dati cifrati.

2. Strumenti di decrittazione

- **Pro:**
 - Possono recuperare i file cifrati senza pagare il riscatto.
 - Alcuni strumenti sono disponibili gratuitamente.
- **Contro:**
 - Non sempre esistono strumenti di decrittazione per tutte le varianti di ransomware.
 - L'uso di questi strumenti richiede competenze tecniche specifiche.

3. Non pagare il riscatto

- **Pro:**
 - Evita di finanziare ulteriori attività criminali.
 - Non c'è garanzia che i file vengano effettivamente decrittati dopo il pagamento.
- **Contro:**
 - Se non ci sono backup disponibili, i dati potrebbero essere persi permanentemente.
 - La pressione di dover recuperare dati critici può essere alta.

4. Analisi forense

- **Pro:**
 - Identifica come è avvenuta l'infezione, aiutando a prevenire futuri attacchi.
 - Fornisce un quadro chiaro dell'impatto dell'infezione.
- **Contro:**

- Può essere costoso e richiedere tempo.
- Richiede competenze specializzate.

2. Misure preventive:

1. Aggiornamenti del sistema

- **Pro:**
 - Risolve le vulnerabilità note, come quella sfruttata da WannaCry.
 - Mantiene il sistema protetto da altre minacce emergenti.
- **Contro:**
 - Gli aggiornamenti possono causare problemi di compatibilità con software più vecchi.
 - Possono richiedere tempo e risorse, soprattutto in grandi infrastrutture.

2. Backup regolari

- **Pro:**
 - Garantisce la possibilità di ripristinare i dati senza dover pagare un riscatto.
 - Riduce il rischio di perdita di dati.
- **Contro:**
 - Richiede spazio di archiviazione aggiuntivo e gestione dei backup.
 - I backup devono essere gestiti correttamente per evitare che anch'essi vengano infettati.

3. Antivirus e software di sicurezza

- **Pro:**
 - Fornisce una protezione in tempo reale contro vari tipi di malware.
 - Molti antivirus sono in grado di rilevare e bloccare WannaCry.
- **Contro:**
 - Nessun software antivirus offre una protezione al 100%.
 - Può rallentare le prestazioni del sistema.

4. Disabilitare SMBv1

- **Pro:**
 - Elimina una delle vulnerabilità critiche sfruttate da WannaCry.
 - Migliora la sicurezza complessiva della rete.
- **Contro:**
 - Alcuni vecchi dispositivi o software potrebbero ancora dipendere da SMBv1.
 - La disabilitazione potrebbe richiedere test e aggiornamenti.

5. Consapevolezza e formazione

- **Pro:**
 - Riduce il rischio di infezioni causate da errori umani, come cliccare su link sospetti.
 - Migliora la cultura della sicurezza all'interno dell'organizzazione.

- **Contro:**
 - Richiede tempo e risorse per formare il personale.
 - L'efficacia dipende dall'adesione e dall'attenzione continua degli utenti.

In sintesi

La migliore difesa contro il ransomware come WannaCry è la prevenzione: aggiornamenti regolari, backup sicuri, e una buona igiene informatica. Se nonostante le precauzioni vieni infettato, agire rapidamente per isolare l'infezione e ripristinare i dati da un backup può limitare i danni.