1. Intervento tempestivo sul sistema infetto:

- Isolo immediatamente il computer infetto dalla rete aziendale per prevenire la diffusione del malware WannaCry ad altri sistemi.
- Disconnetto il computer infetto dalla connessione Internet per impedire la comunicazione del malware con server esterni.
- Avvio una scansione antivirus completa sul sistema infetto per identificare e rimuovere il malware WannaCry.

2. Possibilità di messa in sicurezza del sistema:

a. Aggiornamento del sistema operativo:

- Pro: Aggiornare il sistema operativo Windows 7 alla versione più recente (Windows 10) per ottenere le ultime patch di sicurezza e correzioni di vulnerabilità.
- Contro: Potrebbe richiedere un'implementazione complessa e richiedere il controllo della compatibilità del software esistente con la nuova versione di Windows.

b. Applicazione di patch di sicurezza:

- Pro: Applicare le patch di sicurezza più recenti disponibili per Windows 7, comprese quelle specifiche per mitigare la vulnerabilità utilizzata dal malware WannaCry.
- Contro: Le patch potrebbero non essere più disponibili per Windows 7, poiché il sistema operativo ha raggiunto la fine del supporto esteso nel gennaio 2020.

c. Utilizzo di soluzioni di sicurezza aggiuntive:

- Pro: Implementare soluzioni di sicurezza aggiuntive come firewall avanzati, sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS) per rafforzare la sicurezza complessiva del sistema.
- Contro: Queste soluzioni potrebbero richiedere investimenti aggiuntivi e configurazioni complesse.

d. Educazione degli utenti e sensibilizzazione alla sicurezza:

- Pro: Fornire formazione agli utenti aziendali sulla sicurezza informatica, inclusa l'identificazione di e-mail di phishing e comportamenti online rischiosi.
- Contro: Richiede tempo e risorse per l'implementazione e può richiedere sforzi continui per mantenere l'attenzione degli utenti sulla sicurezza.

e. Backup e ripristino dei dati:

- Pro: Eseguire regolarmente il backup dei dati critici del sistema e implementare un piano di ripristino dei dati in caso di attacchi ransomware o perdita dei dati.
- Contro: Il ripristino dei dati potrebbe richiedere tempo, specialmente se non sono state effettuate regolari copie di backup.

Ogni possibilità sopra elencata deve essere valutata in base alle specifiche esigenze e vincoli dell'azienda, come budget, tempo e risorse disponibili. La combinazione di più misure di sicurezza potrebbe essere necessaria per garantire una protezione efficace del sistema.