W14D2 - NICHOLAS DI ANGELO -

---

1. Intervento tempestivo sul sistema infetto

Passaggi immediati:

1. **Isolamento del sistema infetto**
   - **Azione:** Disconnettere immediatamente il computer infetto dalla rete (sia cablata che Wi-Fi).
   - **Motivazione:** Impedire la diffusione del malware ad altri sistemi all'interno della rete aziendale.
2. **Spegnimento del computer**
   - **Azione:** Spegnere il computer per fermare l'attività del malware.
   - **Motivazione:** Interrompere l'esecuzione del malware per prevenire ulteriori danni.
3. **Notifica alle parti interessate**
   - **Azione:** Informare il team IT, il management e gli utenti interessati dell'infezione.
   - **Motivazione:** Garantire che tutti siano consapevoli del problema e possano collaborare per risolverlo.

---

2. Elenco delle possibilità di messa in sicurezza del sistema

Possibilità 1: Ripristino da backup

Descrizione: Utilizzare un backup precedente non infetto per ripristinare il sistema.

Pro:

- **Sicurezza:** Ripristino del sistema a uno stato sicuramente non infetto.
- **Velocità:** Tempo relativamente breve per il ripristino, se i backup sono aggiornati.
- **Dati integri:** Recupero dei dati fino all'ultimo backup.

Contro:

- **Perdita di dati:** Potenziale perdita dei dati creati dopo l'ultimo backup.
- **Affidabilità:** Necessità di avere un backup funzionante e non corrotto.

Possibilità 2: Rimozione manuale del malware

Descrizione: Utilizzare strumenti antivirus e antimalware per identificare e rimuovere WannaCry dal sistema infetto.

Pro:

- **Costo:** Minori costi rispetto a un ripristino completo o alla reinstallazione.
- **Dati preservati:** Conservazione dei dati attuali se la rimozione è efficace.

Contro:

- **Complessità:** Processo complesso e rischio di non riuscire a rimuovere completamente il malware.
- **Tempo:** Richiede tempo e risorse tecniche elevate.
- **Incertezza:** Possibilità che rimangano tracce del malware nel sistema.

Possibilità 3: Reinstallazione del sistema operativo

Descrizione: Formattare il disco rigido e reinstallare Windows 7 da zero.

Pro:

- **Pulizia completa:** Eliminazione totale del malware con la formattazione del disco.
- **Affidabilità:** Ripartenza da una base pulita e sicura.

Contro:

- **Tempo e risorse:** Processo lungo che richiede reinstallazione di software e riconfigurazione del sistema.
- **Perdita di dati:** Necessità di backup dei dati prima della formattazione per evitare perdite.

Possibilità 4: Aggiornamento del sistema operativo

Descrizione: Aggiornare il sistema operativo a una versione più recente (es. Windows 10) che include patch di sicurezza contro WannaCry.

Pro:

- **Sicurezza:** Sistemi operativi più recenti sono meno vulnerabili a WannaCry.
- **Aggiornamenti:** Accesso a patch di sicurezza e miglioramenti continui.

Contro:

- **Compatibilità:** Possibili problemi di compatibilità con software esistenti.
- **Costo:** Potenziale necessità di nuove licenze software e hardware aggiornato.
- **Formazione:** Necessità di formazione per gli utenti sul nuovo sistema operativo.

---

3. Valutazione dei pro e dei contro di ogni possibilità

Ripristino da backup

- **Pro:** Rapido e sicuro se i backup sono aggiornati.
- **Contro:** Perdita di dati non ancora salvati.

Rimozione manuale del malware

- **Pro:** Conserva i dati attuali, meno costoso.
- **Contro:** Alta complessità e rischio di fallimento.

Reinstallazione del sistema operativo

- **Pro:** Sicurezza garantita, sistema pulito.
- **Contro:** Processo lungo e perdita di configurazioni e dati non salvati.

Aggiornamento del sistema operativo

- **Pro:** Maggiore sicurezza a lungo termine.
- **Contro:** Potenziale incompatibilità e costi associati.

Conclusione

In base alla gravità dell'infezione e alle risorse disponibili, la strategia migliore può variare. Il ripristino da backup è l'opzione più sicura e veloce se i backup sono aggiornati. La rimozione manuale del malware potrebbe essere tentata se i dati recenti non sono stati salvati, ma presenta rischi significativi. La reinstallazione del sistema operativo garantisce la massima sicurezza, ma richiede tempo e preparazione. L'aggiornamento del sistema operativo è consigliabile per migliorare la sicurezza a lungo termine, ma potrebbe comportare costi aggiuntivi e problemi di compatibilità.

La scelta finale dipenderà dalla specifica situazione aziendale, dalla disponibilità dei backup e dalle risorse tecniche a disposizione.

Relazione: Procedura di Messa in Sicurezza del Sistema Windows 7 Infetto da Malware WannaCry – Aggiornamento S.O. – Antivirus - Antimalware

---

1. Introduzione

Questa relazione descrive le azioni intraprese per mettere in sicurezza un computer aziendale con sistema operativo Windows 7 infettato dal malware WannaCry. Verranno illustrati i passaggi iniziali per contenere l'infezione e le varie opzioni di sicurezza adottabili, con una valutazione dei relativi pro e contro.

2. Intervento Tempestivo sul Sistema Infetto

2.1. Isolamento del Sistema

1. **Disconnessione dalla rete**:
   - Il sistema infetto è stato immediatamente disconnesso dalla rete aziendale per prevenire la propagazione del malware ad altri dispositivi.
2. **Segnalazione dell'infezione**:
   - Informato il personale responsabile della sicurezza informatica dell'azienda.
   - Segnalato l'incidente agli utenti per evitare ulteriori interazioni con il sistema infetto.

2.2. Identificazione e Analisi del Malware

1. **Conferma dell'infezione**:
   - Eseguita un'analisi preliminare per confermare che si tratta del malware WannaCry.
2. **Documentazione**:
   - Raccolte informazioni dettagliate sull'infezione, compresi log di sistema e schermate di messaggi di riscatto.

3. Messa in Sicurezza del Sistema

3.1. Possibilità di Ripristino e Sicurezza

Opzione 1: Ripristino da Backup

Procedura:

- Ripristino del sistema da un backup precedente all'infezione.

Pro:

- Rapido ripristino delle funzionalità normali.
- Nessun rischio di rimanenza del malware.

Contro:

- Necessità di avere backup recenti e integri.
- Potenziale perdita di dati non inclusi nel backup.

Opzione 2: Reinstallazione del Sistema Operativo

Procedura:

- Formattazione del disco rigido e reinstallazione di Windows 7.

Pro:

- Eliminazione completa del malware.
- Sistema operativo pulito e privo di residui di infezioni.

Contro:

- Processo lungo e potenzialmente complesso.
- Necessità di reinstallare e configurare tutte le applicazioni.

Opzione 3: Rimozione del Malware con Software di Sicurezza

Procedura:

- Utilizzo di software antivirus e antimalware per rilevare e rimuovere WannaCry.

Pro:

- Minimo impatto sul lavoro quotidiano.
- Conservazione dei dati e delle impostazioni correnti.

Contro:

- Possibile inefficacia se il malware ha compromesso profondamente il sistema.
- Rischio di residui di malware.

3.2. Installazione di Antivirus e Antimalware

Indipendentemente dall'opzione scelta per la messa in sicurezza, è fondamentale installare e configurare software antivirus e antimalware per prevenire future infezioni.

Passaggi:

1. **Scelta del software**:
    - Selezione di un antivirus affidabile (es. Microsoft Security Essentials).
    - Selezione di un software antimalware efficace (es. Malwarebytes).
2. **Installazione**:
    - Download e installazione dei software selezionati.
    - Esecuzione degli aggiornamenti delle definizioni di virus e malware.
3. **Configurazione**:
    - Impostazione di scansioni programmate regolari.

- Configurazione di protezione in tempo reale.

3.3. Aggiornamento del Sistema Operativo

Per prevenire vulnerabilità future, è essenziale mantenere il sistema operativo aggiornato.

Passaggi:

1. **Connessione a Windows Update**:
   - Accesso a "Pannello di controllo" > "Windows Update".
   - Verifica e installazione di tutti gli aggiornamenti disponibili.
2. **Applicazione di patch di sicurezza**:
   - Assicurarsi che tutte le patch critiche, in particolare quelle relative a vulnerabilità note come EternalBlue, siano installate.

4. Valutazione Finale

Dopo aver implementato una delle opzioni di ripristino e messo in sicurezza il sistema, è importante effettuare una valutazione finale per assicurarsi che tutte le minacce siano state eliminate e che il sistema sia adeguatamente protetto per il futuro.

5. Conclusione

Mettere in sicurezza un sistema infetto da WannaCry richiede un intervento immediato e l'adozione di misure preventive. L'azienda deve mantenere pratiche di backup regolari, aggiornare costantemente il software e formare il personale sulla sicurezza informatica per prevenire future infezioni.

Questa relazione è stata preparata per fornire una guida completa e dettagliata sulla messa in sicurezza del sistema infetto e per aiutare a prevenire incidenti simili in futuro.

Chiusura della Porta Vulnerabile SMB

Per evitare future infezioni da malware che sfruttano la vulnerabilità del protocollo SMB (Server Message Block), è necessario disabilitare SMBv1.

Passaggi:

1. **Disabilitare SMBv1 tramite il Pannello di Controllo**:
   - Accedere a "Pannello di controllo" > "Programmi e funzionalità".
   - Cliccare su "Attivazione o disattivazione delle funzionalità di Windows".
   - Scorrere verso il basso fino a trovare "Supporto per condivisione file SMB 1.0/CIFS" e deselezionare questa opzione.
   - Cliccare su "OK" e riavviare il computer se richiesto.
2. **Disabilitare SMBv1 tramite il prompt dei comandi**:
   - Aprire il prompt dei comandi come amministratore.

- Eseguire il comando: `sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi`
- Eseguire il comando: `sc.exe config mrxsmb10 start= disabled`
- Riavviare il computer.

Disabilitare SMBv1 riduce notevolmente il rischio di attacchi simili in futuro.