Report Wannacry

Intervento Tempestivo sul Sistema Infetto:

- Isolamento del Sistema Infetto: La prima azione è isolare il computer infetto dalla rete per prevenire la diffusione del malware ad altri dispositivi. Ciò può essere fatto disconnettendo il computer dalla rete o utilizzando strumenti di sicurezza di rete per isolare il traffico dannoso.
- Analisi del Malware: È essenziale identificare la natura e l'estensione del malware WannaCry sul sistema infetto. Gli strumenti di sicurezza e gli specialisti IT possono essere impiegati per analizzare il codice dannoso e determinare il modo migliore per rimuoverlo.
- Rimozione del Malware: Una volta identificato il malware, è necessario procedere con la sua rimozione completa dal sistema. Questo può essere fatto utilizzando software antivirus aggiornati o strumenti di rimozione malware specifici.

Elenco delle Possibilità di Messa in Sicurezza:

- Aggiornamento del Sistema Operativo: Una delle prime azioni dovrebbe essere l'aggiornamento del sistema operativo a una versione più recente e supportata, come Windows 10, che offre patch di sicurezza per proteggersi da vulnerabilità come WannaCry.
- Installazione di Patch di Sicurezza: Se l'aggiornamento del sistema operativo non è immediatamente possibile, è necessario applicare tutte le patch di sicurezza disponibili per Windows 7, comprese quelle specifiche per mitigare le vulnerabilità sfruttate da WannaCry.
- Implementazione di Soluzioni di Sicurezza Aggiuntive: L'installazione di software antivirus/antimalware aggiornati e firewall aggiuntivi può contribuire a rafforzare la sicurezza del sistema e prevenire futuri attacchi.
- Backup dei Dati: Eseguire backup regolari dei dati critici del sistema su dispositivi esterni o in cloud per garantire la disponibilità e l'integrità dei dati in caso di attacchi malware o altre emergenze.
- Sensibilizzazione e Formazione del Personale: Educare gli utenti sull'importanza della sicurezza informatica e fornire formazione su come riconoscere e evitare le minacce online può contribuire a ridurre il rischio di futuri attacchi.

Valutazione dei Pro e dei Contro di Ogni Possibilità:

- **Aggiornamento del Sistema Operativo:**

1. Pro: Aggiornare il sistema operativo a una versione supportata offre una protezione migliore contro le minacce di sicurezza.

2. Contro: Potrebbe richiedere tempo e risorse per l'aggiornamento e la migrazione dei dati. Alcune applicazioni legacy potrebbero non essere compatibili con le versioni più recenti del sistema operativo.

- **Installazione di Patch di Sicurezza:**

1. Pro: Applicare le patch di sicurezza può mitigare le vulnerabilità e proteggere il sistema da attacchi noti come WannaCry.
2. Contro: Alcune patch potrebbero causare problemi di compatibilità con determinati software o configurazioni di sistema.

- Implementazione di Soluzioni di Sicurezza Aggiuntive:

1. Pro: Aggiungere strati di sicurezza aggiuntivi può aumentare la resilienza del sistema contro attacchi malware.
2. Contro: L'implementazione di soluzioni di sicurezza aggiuntive può comportare costi aggiuntivi e potenziali rallentamenti delle prestazioni del sistema.

- Backup dei Dati:

1. Pro: Eseguire backup regolari dei dati critici riduce il rischio di perdita di dati in caso di attacchi informatici o guasti hardware.
2. Contro: La gestione dei backup richiede tempo e risorse, e i backup non protetti possono essere anch'essi vulnerabili a attacchi ransomware.

- Sensibilizzazione e Formazione del Personale:

1. Pro: Un personale ben informato è una difesa fondamentale contro le minacce informatiche, riducendo il rischio di successo degli attacchi di phishing e di altre tattiche di ingegneria sociale.
2. Contro: La formazione del personale può richiedere tempo e risorse, e potrebbe non eliminare completamente il rischio di errore umano.

WannaCry utilizza la vulnerabilità conosciuta come EternalBlue, che sfrutta una falla nel protocollo Server Message Block (SMB) v1 su Windows. Questa vulnerabilità è stata identificata con la sigla MS17-010 da Microsoft. Dettagli della Vulnerabilità • Nome della Vulnerabilità: EternalBlue

• Identificativo CVE: CVE-2017-0144

• Protocollo Interessato: SMBv1 (Server Message Block versione 1)

• Patch di Sicurezza: MS17-010

• Descrizione: EternalBlue sfrutta una vulnerabilità nei servizi SMB di Windows che consente a un attaccante remoto di eseguire codice arbitrario sul sistema target senza autenticazione. Questo permette di installare programmi, visualizzare, cambiare o eliminare dati, o creare nuovi account con pieni diritti di amministratore.

Raccomandazioni per il futuro:

- ☐ Eseguire periodicamente Vulnerability Assessment
- ☐ Segmentazione della Rete: - Applicare la segmentazione della rete per limitare il movimento laterale delle minacce. Utilizzare VLAN e altre tecniche di segmentazione per isolare i segmenti di rete critici.
- ☐ Settare regole del firewall, soprattutto su porte 445, 139 e 3389
- ☐ Policy di Controllo degli Accessi: - Applicare rigorose policy di controllo degli accessi, assicurando che gli utenti abbiano accesso solo ai dati necessari per i loro ruoli.