Traccia: infezione malware

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?

Consegna:

- Per prima cosa occorre intervenire tempestivamente sul sistema infetto
- In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
- Per ogni possibilità valutare i pro e i contro

Remediation dell'Infezione da WannaCry su PC Windows 7

Data del Report: 22/05/2024

Redatto da: Elisa B.

Sistema Affetto: PC Windows 7

Minaccia Rilevata: Ransomware WannaCry

Il giorno 22/05/2024, un PC Windows 7 all'interno della nostra rete è stato identificato come infettato dal ransomware WannaCry. Sono state prese immediatamente misure per isolare il sistema infetto e mitigare la diffusione del ransomware all'interno della nostra rete aziendale. Questo report descrive i passi di remediation intrapresi per mettere in sicurezza il sistema infetto e la rete, insieme a strategie a lungo termine per migliorare la sicurezza generale.

Azioni Immediate di Remediation

1. Isolamento del Sistema Infetto:

- Il PC infetto è stato immediatamente scollegato da tutte le connessioni di rete (sia cablate che wireless) per evitare la diffusione del ransomware.

2. Backup dei Dati:

- Dove possibile, sono stati eseguiti backup dei dati non infetti su un supporto esterno. Il backup è stato messo in sicurezza e isolato dalla rete per ulteriori ispezioni.

3. Formattazione e Reinstallazione del Sistema:

- L'hard disk del PC infetto è stato formattato per garantire la rimozione completa del ransomware.

- È stata eseguita una nuova installazione di Windows 7 (nonostante sia stato segnalato, che l'upgrade alla versione 10 o 11 di Windows, eviterebbe l'esposizione futura al Worm WannaCry e lo sfruttamento della vulnerabilità EternalBlue) utilizzando un supporto di installazione sicuro e verificato.

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.

---

4. Installazione delle Patch di Sicurezza:

- Dopo la reinstallazione, sono state scaricate e installate tutte le patch di sicurezza disponibili per Windows 7, con particolare attenzione alla patch MS17-010 che corregge la vulnerabilità sfruttata da WannaCry.

5. Installazione e Scansione Antivirus:

- È stata installata una soluzione antivirus affidabile e aggiornata sul sistema pulito.

- È stata condotta una scansione completa del sistema per confermare la rimozione di eventuali malware residui.

Misure di Sicurezza a Livello di Rete

1. Aggiornamento di Tutti i Sistemi:

- Tutti i sistemi all'interno della rete sono stati aggiornati con le ultime patch di sicurezza, concentrandosi sulle vulnerabilità sfruttate dai ransomware come MS17-010.

2. Configurazione del Firewall:

- I firewall sono stati configurati per bloccare le porte non necessarie (incluse le porte 445, 139 e 3389) per mitigare i tentativi di sfruttamento.

3. Soluzioni Antivirus e Antimalware:

- Sono state distribuite soluzioni antivirus e antimalware aggiornate su tutti i dispositivi della rete.

- Sono state programmate scansioni regolari per rilevare ed eliminare potenziali minacce.

4. Strategia di Backup:

- È stata implementata una strategia di backup robusta, garantendo backup regolari e automatizzati dei dati critici.

- I backup sono conservati in modo sicuro e separato dall'infrastruttura di rete principale.

5. Segmentazione della Rete:

- È stata applicata la segmentazione della rete per limitare il movimento laterale delle minacce.

- Sono state utilizzate VLAN e altre tecniche di segmentazione per isolare i segmenti di rete critici.

6. Formazione dei Dipendenti:

- È stata condotta una formazione sulla sicurezza informatica per tutti i dipendenti, concentrandosi sul riconoscimento dei tentativi di phishing e sulle pratiche di navigazione sicura.

7.Policy di Controllo degli Accessi:

- Sono state applicate rigorose policy di controllo degli accessi, assicurando che gli utenti abbiano accesso solo ai dati necessari per i loro ruoli.

8. Monitoraggio e Risposta agli Incidenti:

- È stato implementato il monitoraggio continuo della rete per rilevare attività anomale.

- È stato sviluppato e testato un piano di risposta agli incidenti per gestire efficacemente eventuali futuri attacchi informatici.

9. Audit di Sicurezza Periodici:

- Sono stati programmati audit di sicurezza e valutazioni di vulnerabilità regolari per identificare e affrontare potenziali lacune di sicurezza.

Raccomandazioni a Lungo Termine

Aggiornamento del Sistema:

- Considerare l'aggiornamento di tutti i sistemi Windows 7 a una versione più recente e supportata, come Windows 10, per beneficiare degli aggiornamenti di sicurezza continui.

Conclusione

La minaccia immediata posta dall'infezione da ransomware WannaCry è stata contenuta e mitigata con successo. Sono state implementate misure complete per mettere in sicurezza il PC infetto e la rete aziendale. Andando avanti, il nostro focus rimarrà sulle pratiche di sicurezza proattive, sul monitoraggio continuo e sugli aggiornamenti regolari ai nostri sistemi e policy per prevenire future minacce.

Questo report fornisce un resoconto dettagliato delle azioni intraprese e dei piani implementati per garantire la sicurezza e l'integrità della nostra rete in risposta all'incidente di ransomware WannaCry.