ESERCIZIO W14D1 PRATICA 2

Report sull'Infezione da WannaCry e Misure di Sicurezza

---

1. Introduzione

L'azienda che segui come consulente di sicurezza è stata colpita da un'infezione da malware WannaCry su un computer con sistema operativo Windows 7. Questo tipo di malware è noto per la sua capacità di diffondersi rapidamente attraverso la rete, criptando i file delle vittime e richiedendo un riscatto per il loro sblocco. È essenziale agire tempestivamente per contenere e risolvere questa minaccia, proteggendo così l'azienda da danni maggiori.

2. Azioni Immediate

Prima di tutto, è fondamentale intervenire rapidamente sul sistema infetto per evitare una diffusione ulteriore del malware e limitare i danni. Le azioni immediate includono:

- **Isolare il dispositivo infetto**: Disconnettere il computer infetto dalla rete per impedire al malware di diffondersi ad altri dispositivi.
- **Scansione antivirus**: Eseguire una scansione completa del sistema con un software antivirus aggiornato per individuare e rimuovere il malware.
- **Scaricare tool di ricerca malware**: Utilizzare un sistema non infetto per scaricare gli strumenti di ricerca malware e trasferirli sul dispositivo infetto tramite una chiavetta USB. Questi strumenti possono individuare e neutralizzare il malware presente.

3. Analisi Approfondita

Dopo aver affrontato l'emergenza, è necessario pianificare e implementare misure di sicurezza più approfondite per prevenire future infezioni e proteggere l'azienda da minacce simili. Le varie possibilità di messa in sicurezza del sistema includono:

- **Analisi del codice malevolo tramite reverse engineering**: Analizzare il codice del malware per comprendere il suo funzionamento e sviluppare contromisure più efficaci.
- **Verifica del backup**: Assicurarsi che sia disponibile un backup recente del sistema per consentire il ripristino dei dati in caso di necessità.
- **Sensibilizzazione degli utenti**: Fornire formazione agli utenti sull'importanza della sicurezza informatica e sulle pratiche consigliate per prevenire infezioni da malware.
- **Limitazione dei privilegi**: Ridurre i privilegi di accesso degli utenti per limitare l'impatto delle potenziali infezioni.
- **Segnalazione agli enti competenti**: Nel caso in cui siano coinvolti dati sensibili o sia stata violata la privacy, fare una segnalazione agli enti competenti per l'indagine e le azioni legali necessarie.

4. Misure Preventive e di Monitoraggio

Per prevenire futuri attacchi e rafforzare la sicurezza complessiva del sistema, è consigliabile implementare le seguenti misure:

- **Monitoraggio dell'attività di rete**: Utilizzare strumenti di monitoraggio per rilevare e bloccare attività sospette sulla rete.
- **Firewall con regole rigide**: Configurare firewall, sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS) con regole rigorose per filtrare il traffico dannoso.
- **Aggiornamenti software e patch di sicurezza**: Mantenere aggiornato il software e applicare regolarmente le patch di sicurezza per correggere le vulnerabilità note.
- **Backup regolari**: Eseguire regolarmente il backup dei dati critici e testare periodicamente la procedura di ripristino.
- **Educazione sulla sicurezza informatica**: Continuare a fornire formazione e sensibilizzazione agli utenti sulla sicurezza informatica e sulle migliori pratiche da seguire.

5. Conclusioni

In conclusione, l'infezione da malware WannaCry rappresenta una seria minaccia per l'azienda, ma è possibile affrontarla con una combinazione di azioni immediate e misure preventive a lungo termine. È fondamentale agire con tempestività, analizzare attentamente il malware e implementare una strategia completa di sicurezza informatica per proteggere l'azienda da future minacce.

Questo report fornisce una panoramica delle azioni da intraprendere per affrontare l'infezione da WannaCry e mettere in sicurezza il sistema aziendale. Ogni misura proposta è valutata considerando i suoi vantaggi e svantaggi per garantire un approccio equilibrato alla sicurezza informatica.