Esercizio M4-W2-D2

Daniele Atzori

Infezione Malware WannaCry

Quando si scopre che un computer con Windows 7 è stato infettato dal malware WannaCry, è essenziale intervenire tempestivamente per limitare i danni e mettere in sicurezza il sistema. Il primo passo è isolare immediatamente il computer infetto dalla rete per impedire che il malware si propaghi ad altri dispositivi. Spegnere il Wi-Fi, disconnettere il cavo Ethernet e assicurarsi che non ci siano connessioni di rete attive.

Dopo aver isolato il sistema, una delle prime possibilità di messa in sicurezza è tentare di rimuovere il malware utilizzando software antivirus o antimalware aggiornati. Questa opzione può essere rapida ed efficace se il software di sicurezza è in grado di identificare e rimuovere WannaCry. Tuttavia, il rischio è che il malware abbia già criptato i file o installato altre minacce che non vengono completamente rimosse, lasciando il sistema vulnerabile.

Un'altra possibilità è ripristinare il sistema a uno stato precedente utilizzando punti di ripristino di Windows o backup esistenti. Questa soluzione può riportare il sistema a uno stato funzionante senza malware, ma è efficace solo se i backup sono recenti e non infetti. Un possibile contro è la perdita di dati recenti che non sono stati inclusi nei backup.

La reinstallazione completa del sistema operativo è una misura più drastica ma garantisce la rimozione totale del malware. Dopo aver formattato il disco rigido e reinstallato Windows 7, si può ripristinare i dati da backup sicuri. Questo metodo assicura un sistema pulito, ma è laborioso e richiede tempo, oltre a necessitare di backup completi e affidabili.

Aggiornare il sistema operativo a una versione più recente, come Windows 10, è un'altra opzione da considerare. Windows 7 non è più supportato da Microsoft e non riceve aggiornamenti di sicurezza, rendendolo vulnerabile a nuove minacce. L'aggiornamento a Windows 10 offre migliori protezioni di sicurezza integrate e riduce il rischio di future infezioni. Tuttavia, questa soluzione può comportare costi aggiuntivi e richiede che l'hardware del computer sia compatibile con la nuova versione del sistema operativo.

In parallelo con queste azioni, è fondamentale aggiornare tutti i software e le applicazioni installate, inclusi i driver e i programmi di sicurezza. L'aggiornamento dei software chiave riduce le vulnerabilità sfruttabili dai malware e aumenta la resistenza del sistema contro eventuali attacchi futuri.

Infine, è essenziale educare gli utenti sul riconoscimento e la prevenzione dei malware. Organizzare sessioni di formazione sulla sicurezza informatica, insegnare le pratiche di navigazione sicura e l'importanza degli aggiornamenti regolari contribuisce a creare un ambiente di lavoro più sicuro. Sebbene questo approccio richieda un impegno continuo e risorse per la formazione, è un investimento a lungo termine che può ridurre significativamente il rischio di infezioni malware future.