INDICE

Facoltativo:

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

Nel momento in cui viene identificata la presenza del ransomware WannaCry su un sistema Windows, l'obiettivo primario non è il recupero immediato dei dati, ma il contenimento dell'incidente e la protezione dell'infrastruttura complessiva.
WannaCry è progettato per diffondersi automaticamente all'interno della rete sfruttando vulnerabilità nei servizi di condivisione di Windows; di conseguenza, qualsiasi ritardo nelle azioni iniziali può trasformare un singolo computer compromesso in un evento di sicurezza su scala aziendale.
La prima azione consiste quindi nell'interrompere immediatamente ogni forma di comunicazione del sistema infetto, disconnettendolo dalla rete sia a livello logico sia fisico. Questo isolamento impedisce al malware di propagarsi verso altri dispositivi e consente di stabilizzare la situazione prima di procedere con ulteriori analisi.
Parallelamente all'isolamento, viene attivato il processo di gestione dell'incidente, informando il personale IT e le figure responsabili della sicurezza.
Questa fase è fondamentale per coordinare le attività, evitare interventi non controllati e garantire che le decisioni successive siano prese in modo strutturato.
Quando possibile, prima di qualsiasi intervento distruttivo, viene valutata la possibilità di preservare una copia dei dati presenti sul sistema compromesso, sia per scopi di analisi sia per verificare se esistano file recuperabili.
Tuttavia**, tali operazioni vengono effettuate esclusivamente in modalità offline**, per evitare qualsiasi rischio di ulteriore contaminazione.
Una volta contenuto l'evento, si passa alla valutazione delle diverse strategie di messa in sicurezza del sistema.
La soluzione più affidabile e raccomandata in presenza di ransomware (come WannaCry) è la formattazione completa del computer seguita da una reinstallazione pulita del sistema operativo.
Questo approccio garantisce l'eliminazione totale del malware e di qualsiasi meccanismo di persistenza eventualmente installato, ripristinando un ambiente sicuro e controllato; il principale svantaggio di questa scelta è la perdita dei dati locali non protetti da backup e il tempo necessario per ricostruire il sistema, ma in termini di sicurezza rappresenta l'unica opzione che offre una reale certezza di bonifica.

Un’alternativa è il ripristino del sistema a partire da un backup precedente all’infezione, se sono disponibili copie di sicurezza affidabili e non compromesse, questa opzione consente di recuperare i dati e ridurre i tempi di inattività.
Tuttavia, questa soluzione è sicura solo se si ha la certezza che il backup sia stato effettuato prima dell’attacco e che non contenga già componenti del malware, in caso contrario, il rischio è quello di reintrodurre l’infezione nel sistema ripristinato, vanificando l’intervento.
È inoltre possibile tentare la rimozione del ransomware tramite strumenti specializzati di analisi e disinfezione.
Questa strategia può sembrare più rapida e meno invasiva, ma presenta un rischio significativo: WannaCry e malware simili possono lasciare componenti nascosti o alterare parti del sistema operativo che non vengono completamente ripristinate dagli strumenti di pulizia. Di conseguenza, anche se il ransomware visibile viene rimosso, il sistema potrebbe rimanere instabile o vulnerabile a nuove compromissioni, per questo motivo, in contesti professionali questa opzione viene considerata meno affidabile rispetto alla reinstallazione completa.
Indipendentemente dalla strategia scelta per il ripristino, una fase cruciale è l’aggiornamento del sistema operativo e delle sue componenti di sicurezza.
WannaCry sfrutta vulnerabilità note che sono state corrette dai produttori tramite patch ufficiali; pertanto, prima di rimettere il sistema in rete, è essenziale applicare tutti gli aggiornamenti disponibili e verificare che i servizi di rete vulnerabili siano correttamente protetti o disabilitati.
Solo dopo questa fase il computer può essere reintegrato nell’ambiente operativo.
In conclusione, la gestione di un’infezione da WannaCry richiede un approccio metodico che privilegi il contenimento, l’eliminazione completa della minaccia e il ripristino sicuro dell’operatività. Le decisioni prese in queste fasi determinano non solo la sicurezza del singolo sistema, ma la resilienza dell’intera infrastruttura, rendendo essenziale una valutazione attenta dei rischi e dei benefici associati a ogni possibile strategia di intervento.

CONCLUSIONE

La gestione di un'infezione da WannaCry richiede un approccio strutturato che metta al centro la protezione dell'infrastruttura prima ancora del recupero dei dati.
L'isolamento immediato del sistema compromesso, seguito da una valutazione rigorosa delle opzioni di ripristino, consente di evitare la propagazione del malware e di ridurre l'impatto complessivo dell'incidente.
Le diverse strategie analizzate mostrano come le soluzioni più rapide non siano sempre le più sicure, mentre le procedure più drastiche, come la reinstallazione completa del sistema, garantiscono un livello di affidabilità superiore.
Attraverso questa metodologia operativa emerge l'importanza di combinare prevenzione, risposta agli incidenti e gestione dei backup come elementi fondamentali di una strategia di sicurezza efficace.
Un'infezione da ransomware non rappresenta solo un problema tecnico isolato, ma un evento che mette alla prova l'intera organizzazione, rendendo indispensabile l'adozione di procedure chiare e decisioni basate su criteri di sicurezza e continuità operativa.