Se il computer dell’azienda è stato infettato dal malware WannaCry è importante prendere immediatamente provvedimenti per proteggere il sistema e i dati. WannaCry è stato un ransomware noto per diffondersi rapidamente sfruttando una vulnerabilità in Windows, quindi è essenziale agire prontamente.

WannaCry è un tipo di malware, specificamente un ransomware. Il termine "ransomware" deriva dalla parola inglese "ransom," che significa "ricatto." Questo tipo di malware crittografa i file sul computer infetto e quindi chiede un pagamento alle vittime per ottenere la chiave di decrittazione necessaria per ripristinare i propri file.

La prima cosa che andremo a fare è disconnettere il computer dalla rete Internet e dalla rete locale (se applicabile). Questo aiuterà a prevenire la diffusione del malware ad altri dispositivi nella rete.

Il prima possibile dobbiamo arrestare il sistema così da evitare che il malware possa continuare ad eseguire attività dannose.

Eseguiamo una scansione del SO con un antivirus e seguiamo le istruzioni per rimuovere il malware, inoltre controlliamo che il sistema Win7 sia aggiornato poiché Microsoft ha rilasciato patch di sicurezza per chiudere la vulnerabilità utilizzata da WannaCry chiamata "EternalBlue". Verifichiamo che il sistema abbia tutte le patch di sicurezza installate. Se non lo sono, vanno installate le patch mancanti utilizzando Windows Update; inoltre dobbiamo considerare l'aggiornamento di Windows 7, che non è più supportato da Microsoft con aggiornamenti di sicurezza, con sistemi come Windows 10 o Windows 11, che ricevono aggiornamenti regolari per la sicurezza.

Poi verifichiamo se abbiamo un backup sicuro dei file e se non lo abbiamo proviamo ad utilizzare un dispositivo di archiviazione esterno o un servizio di backup cloud affidabile per cercare i salvare i dati che non sono stati compromessi.

Cambiamo le password dell'account utente sul computer, compresa la password dell'amministratore. Soprattutto, la password dell'account utilizzato per l'accesso amministrativo.

Se la situazione è critica e il computer è stato completamente compromesso, dobbiamo formattare il disco rigido e reinstallare il sistema operativo da zero. Ovviamente verranno persi tutti i dati al suo interno e la possibilità di riuscire a recuperarli sono minime.

N.B. anche se abbiamo file nel pc molto importanti non dobbiamo pagare il riscatto per evitare di incentivare questo genere di crimine, dobbiamo invece denunciare l’accaduto e usarlo come lezione per imparare a stare più attenti alla sicurezza informatica.

Una volta ripristinato il sistema, assicuriamoci di migliorare la sicurezza del computer. Questo include l'installazione di un software antivirus aggiornato, l'uso di un firewall, l'applicazione di patch regolari e l'educazione sulla sicurezza informatica per evitare future infezioni, inoltre sarebbe buona norma avere i file importanti sempre in duplice copia così che anche se una dovesse essere compromessa ne abbiamo un’altra copia, per farlo possiamo usare una memoria esterna come un hard-disk esterno o un buon sistema cloud, nel caso usassimo la memoria fisica dobbiamo considerare di tenerla in un posto ben sicuro e infine dovremmo eseguire periodicamente dei test sulle vulnerabilità presenti nella rete e nei computer dell’azienda con un tecnico così da intervenire preventivamente e limitare i nuovi attacchi.