Report wannacry

1. Isolamento: Isola immediatamente il computer infetto dalla rete per impedire la diffusione del malware ad altri dispositivi. Disconnetti il computer dalla rete cablata o disattiva la connessione Wi-Fi.
2. Rimozione del malware: Utilizza un software antivirus aggiornato per eseguire una scansione completa del sistema infetto. Assicurati che l'antivirus sia dotato di definizioni di virus aggiornate per rilevare e rimuovere WannaCry.
3. Aggiornamenti del sistema operativo: Windows 7 è vulnerabile a WannaCry perché Microsoft ha rilasciato una patch di sicurezza per proteggere i sistemi dall'attacco. Assicurati che il sistema operativo Windows 7 sia completamente aggiornato con gli ultimi aggiornamenti di sicurezza forniti da Microsoft.
4. Disabilita SMBv1: WannaCry sfrutta una vulnerabilità nel protocollo SMBv1 di Windows. Disabilita SMBv1 sul computer infetto per prevenire ulteriori infezioni. Puoi farlo andando nel Pannello di controllo > Programmi > Attiva o disattiva funzionalità di Windows, quindi deselezionare "Supporto per SMB 1.0/CIFS".
5. Backup e ripristino: Verifica che i tuoi dati critici siano stati adeguatamente copiati di recente. Se possibile, formatta il disco rigido del computer infetto e reinstalla il sistema operativo da zero. Successivamente, ripristina i dati da un backup pulito e sicuro.
6. Consapevolezza dell'utente: Educa gli utenti sull'importanza di pratiche sicure, come l'apertura di allegati o link solo da fonti attendibili e l'aggiornamento regolare del software.
7. Miglioramenti della sicurezza: Valuta l'aggiornamento del sistema operativo a una versione più recente supportata, come Windows 10, che fornisce una migliore protezione contro le minacce informatiche. Considera anche l'installazione di software di sicurezza aggiuntivo, come firewall e software di rilevamento delle intrusioni.
8. Monitoraggio: Implementa un sistema di monitoraggio continuo per individuare eventuali attività sospette o tentativi di intrusioni nel futuro.