Esercitazione 6 Modulo 4 – Alessio Russo

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema? Consegna:
• Per prima cosa occorre intervenire tempestivamente sul sistema infetto
• In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
• Per ogni possibilità valutare i pro e i contro

L'attacco di WannaCry sfrutta una vulnerabilità presente in molte versioni di Windows, compresa Windows 7. Per proteggere i nostri dispositivi è innanzitutto necessario avere tutti dispositivi aggiornati; quindi, il primo step sarà aggiornare il sistema operativo.

Dal menu Start e seleziona "Control Panel" -> "System and Security" -> "Windows Update" -> "Check for updates" per verificare la disponibilità degli aggiornamenti. Nel caso ci fossero trovati aggiornamenti da installare per risolvere bug e vulnerabilità di sicurezza sarà necessario cliccare su "Install Updates".

Per proteggersi da WannaCry il quale sfrutta una vulnerabilità presente nella versione obsoleta del protocollo SMB, (SMBv1). Sarà necessario disabilitare questa funzionalità per ridurre il rischio che il virus si diffonda di nuovo. Per fare ciò: Start -> "Turn Windows features on or off" -> "SMB 1.0/CIFS File Sharing Support" una volta trovata questa voce dovrà essere deselezionata per disattivare il protocollo. Successivamente sarà necessario cliccare su "OK" e riavvia il computer

Anche se abbiamo affettato questi step precedenti potrebbe esserci ancora del malware quindi il consiglio è scannerizzare il sistema con software antivirus della software House norton ad esempio Avg, avast installare il software ed effettuare una scansione completa del sistema per rilevare eventuali tracce rimaste.

Inoltre, sarà sicuramente necessario modificare le password in quanto questa operazione sarà sicuramente utile ad evitare la diffusione di virus in futuro.

La soluzione migliore è aggiornare il sistema operativo a Windows 10 o 11. Il primo passaggio è mettere in sicurezza la rete isolando il computer (staccando il cavo di rete oppure disattivando il wifi) ed effettuare la scansione antimalware