REPORT W14D1 – PEPPOLI

Traccia: infezione malware

Esercizio: 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?

WannaCry: cos'è e come agisce

WannaCry è un ransomware noto per la sua capacità di diffondersi rapidamente sfruttando una vulnerabilità nel protocollo SMB di Windows. Una volta infettato un sistema, WannaCry crittografa i file dell'utente e richiede un pagamento di riscatto in cambio della chiave di decrittazione.

Isolare dispositivo infetto

Dopo aver scoperto l'infezione da WannaCry, la prima azione intrapresa è stata isolare il dispositivo infetto dalla rete aziendale per prevenire la diffusione del ransomware ad altri sistemi.

Scansione antivirus

È stata eseguita una scansione antivirus completa sul dispositivo infetto per individuare e rimuovere qualsiasi traccia del malware WannaCry.

Scaricare tool di ricerca malware e analisi del codice malevolo

Dato che il dispositivo infetto era un sistema Windows 7, sono stati scaricati strumenti di ricerca malware da un sistema non infetto e trasferiti tramite una chiavetta USB per eseguire ulteriori scansioni e identificare eventuali file malevoli. È stata anche condotta un'analisi del codice malevolo tramite reverse engineering per comprendere meglio il funzionamento del malware e individuare eventuali punti deboli.

Verificare la presenza di backup e sensibilizzazione degli utenti

È stata verificata l'esistenza di backup regolari dei dati aziendali al fine di ripristinare il sistema operativo prima dell'attivazione del file malevolo. Inoltre, è stata condotta una sessione di sensibilizzazione degli utenti sull'importanza della sicurezza informatica e delle best practice da seguire per prevenire future infezioni da malware.

Limitazione dei privilegi e monitoraggio delle attività di rete

Sono state implementate misure per limitare i privilegi degli utenti e monitorare attentamente le attività di rete per individuare eventuali comportamenti anomali che potrebbero indicare un'ulteriore infezione da malware.

Firewall e aggiornamenti software

È stato potenziato il firewall aziendale con regole più rigide, inclusi sistemi di rilevamento delle intrusioni (IDS) e di prevenzione delle intrusioni (IPS), per bloccare eventuali tentativi di accesso non autorizzato. Inoltre, sono stati effettuati aggiornamenti software regolari e applicate patch di sicurezza per mitigare le vulnerabilità del sistema operativo e delle applicazioni.

Remediation:

Backup a cadenza regolare

Sono state implementate procedure di backup regolari per garantire la disponibilità e l'integrità dei dati aziendali in caso di futuri attacchi ransomware o altri incidenti.

Educazione sulla sicurezza informatica

Sono state condotte sessioni di formazione per sensibilizzare gli utenti sulle best practice della sicurezza informatica e sulle potenziali minacce online.

Uso di proxy

È stato implementato un server proxy per filtrare e controllare il traffico Internet al fine di proteggere la rete aziendale da minacce esterne.

Test di vulnerabilità e pen test

Sono stati eseguiti regolarmente test di vulnerabilità e penetration test per identificare e risolvere eventuali debolezze nella sicurezza dei sistemi e delle reti aziendali.

Monitoraggio delle vulnerabilità

È stato istituito un processo continuo di monitoraggio delle vulnerabilità per identificare e risolvere rapidamente le vulnerabilità del sistema prima che possano essere sfruttate da attaccanti malintenzionati.