**RESTART: resilienza e formazione per le PMI**

**Studio di caso**

**(Risultato del progetto 3 - Compito 3.1 e Compito 3.2)**

|  |  |
| --- | --- |
| **Autore del caso di studio:** | Internet Web Solutions |
| **Nome del modulo a cui è assegnato il caso di studio:** | Modulo 3: Cybersecurity nell'ufficio (domestico) |
| **Titolo del caso di studio:** | WannaCry: l'importanza degli aggiornamenti |
| **Descrizione del caso di studio:** | L'Agenzia dell'Unione europea per la sicurezza informatica ha riportato nel maggio 2017 il primo caso di cooperazione informatica a livello europeo, in cui ha collaborato con diversi Stati membri utilizzando le procedure operative standard dell'UE. Tuttavia, questa cooperazione è stata innescata da una situazione complicata generata da un massiccio ransomware.  Secondo la formazione RESTART, un ransomware è un pericoloso tipo di malware che cripta i file sul disco rigido del dispositivo e limita l'accesso all'utente, chiedendo un riscatto, solitamente in criptovalute, in cambio della decriptazione dei file.  **Cosa è successo?**  Venerdì 12 maggio 2017 si è verificato un evento che ha colpito migliaia di computer in tutto il mondo: l'attacco ransomware "WannaCry". Solo nelle prime ore dell'attacco, sono stati colpiti più di 190.000 computer in 150 paesi, tra cui settori e operatori di infrastrutture critiche come sanità, trasporti, istruzione, energia, finanza e telecomunicazioni, e impianti di produzione in diversi paesi dell'UE hanno subito danni alle loro intere linee di produzione.  Questo è avvenuto dopo che sugli schermi dei loro computer è apparso un messaggio che indicava che i loro sistemi e i loro file sarebbero stati bloccati fino al pagamento di un riscatto.  **Perché è successo?**  WannaCry ha colpito i dispositivi del sistema operativo Microsoft Windows sfruttando la vulnerabilità MS17-010 attraverso il codice "EternalBlue" utilizzato dagli hacker.  Sebbene il ransomware richieda solitamente l'interazione dell'utente con qualcosa, come il download di un allegato e-mail infetto o la visita di un sito web che scarica il malware sul dispositivo, WannaCry richiedeva solo che il dispositivo avesse la versione vulnerabile di Windows per essere infettato.  La diffusione è stata molto rapida in quanto utilizzava un protocollo chiamato "SMBv1" che comunicava con stampanti e dispositivi collegati alla stessa rete per continuare a infettare, e principalmente rendeva inaccessibili i file e bloccava i programmi del computer, chiedendo un riscatto in cambio del ripristino delle normali attività.  **Come si sarebbe potuto evitare?**  Oggi sappiamo che quando è successo tutto questo, Windows aveva già una versione aggiornata che risolveva la vulnerabilità sfruttata da Wannacry. Pertanto, il modo più semplice per evitarlo sarebbe stato quello di disporre degli ultimi aggiornamenti di sicurezza e di un antivirus aggiornato. Inoltre, anche altre misure contribuiscono a rendere l'impatto minore o inesistente:   * Eseguire regolarmente il backup di tutti i file. * Conduzione di campagne di sensibilizzazione sulla cybersicurezza con i dipendenti. * In caso di infezione, non pagate il riscatto, ma contattate l'assistenza di un esperto, poiché il pagamento non garantisce che gli utenti siano in grado di accedere nuovamente ai loro file. |
| **Link per ulteriori informazioni:** | <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> |
| **Gruppo target dello studio di caso:** | Micro, piccole e medie imprese (MPMI)  Dipendenti delle MPMI  L'ecosistema IFP dell'UE  Organizzazioni di supporto alle imprese |
| **ESCO competencies and skills** | |
| 1. Capacità e competenze trasversali 2. Abilità sociali ed emotive 3. Pensiero critico 4. Pensiero analitico 5. Risoluzione dei problemi 6. Autogestione 7. Gestione aziendale 8. Adattabilità 9. Resilienza 10. Creatività 11. Networking 12. Iniziativa 13. Flessibilità 14. Apertura 15. Comprendere la complessità 16. Cooperazione 17. Empatia 18. Innovazione 19. Leadership      1. Abilità 2. Competenze tecnologiche 3. Marketing del prodotto 4. Marketing digitale 5. Competenze digitali 6. Comunicazione 7. Cooperazione 8. Intelligenza emotiva      1. Conoscenza 2. Gestione aziendale 3. Apprendimento e formazione online 4. Pubblicità 5. Cloud computing 6. Big data 7. E-commerce 8. Intelligenza artificiale 9. Sacco 10. Alfabetizzazione digitale 11. Sicurezza informatica 12. Data mining e analisi 13. Sostenibilità 14. Benessere 15. Cambiamento climatico 16. Gestione dei social media | |