**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:** | Phishing + SMS: i rischi dello smishing |
| **Descrizione del caso di studio:** | Come già sapete dal modulo " Cybersecurity nell'ufficio (domestico)", il phishing è l'attacco più comune alle PMI europee, e può variare a seconda del metodo utilizzato per l'attacco. In questo caso di studio ci concentriamo sullo smishing, la tecnica di phishing via SMS.  Questo caso di studio è stato estratto dall'Istituto Nazionale di Cybersecurity in Spagna (INCIBE), che fornisce una serie di storie reali relative alla cybersecurity come misura per sensibilizzare le aziende sull'importanza di adottare le necessarie misure di emergenza.  **Che cosa è successo?**  Un dipendente del reparto amministrativo di una PMI era incaricato di gestire la ricezione e l'invio dei pacchi dell'azienda attraverso i servizi di diversi corrieri. Ogni giorno vengono spediti e ricevuti pacchi in azienda, quindi questo dipendente stava aspettando una scatola con materiali per il reparto di produzione.  Quel giorno, il dipendente ha ricevuto un SMS sul suo smartphone aziendale da quella che sembrava essere una società di consegna pacchi. L'SMS indicava che era necessario scaricare un'applicazione tramite un link fornito nel messaggio, al fine di gestire la consegna, così il dipendente ha proceduto a farlo.  Giorni dopo, i colleghi incaricati del pagamento delle bollette hanno avvisato il dipendente che la sua bolletta telefonica aziendale era molto più alta del solito. Questo perché dal dispositivo era stato inviato un numero elevato di SMS durante tutto il mese, senza che il dipendente ne fosse a conoscenza.  **Perché è successo?**  Il dipendente è stato vittima di smishing. L'SMS proveniva da un mittente falso e, cliccando sul link e scaricando l'app, aveva infettato il suo telefono con il malware "FluBot", un trojan che si installa sui dispositivi Android con l'obiettivo di rubare informazioni bancarie spacciandosi per una società di consegna pacchi che invita ad agire immediatamente per evitare di perdere il pacco. Inoltre, il malware utilizza la rubrica del telefono per inviare altri falsi messaggi SMS e infettare più dispositivi, esegue comandi in remoto e impedisce all'utente di disinstallare l'applicazione.  **Come si sarebbe potuto evitare?**  Sebbene il telefono del dipendente sia stato infine ripristinato dal reparto IT dell'azienda, tutto ciò avrebbe potuto essere evitato con misure quali:   * Implementando le politiche di cybersecurity in azienda per controllare e limitare l'uso dei dispositivi aziendali e delle applicazioni installate. * Non installarando applicazioni da fonti sconosciute. * Diffidarando dei messaggi che includono link o allegati. * - Avere attivato e aggiornato tutti gli aggiornamenti di sicurezza del sistema operativo e dell'antivirus. |
| **Link per ulteriori informazioni:** | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms> |
| **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 |
| **Competenze e abilità delle ESCO** | |
| 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 | |