**RESTART: Reziliencia és képzés a kkv-k számára**

**Esettanulmány**

**(3. Projekteredmény - 3.1. Feladat & 3.2 Feladat)**

|  |  |
| --- | --- |
| **Az esettanulmány szerzője:** |  Internet Web Solutions |
| **Annak a modulnak a neve, amelyhez az esettanulmány tartozik:**  |  3. modul: Kiberbiztonság otthon és az irodában  |
| **Az esettanulmány címe:** | Adathalászat + SMS: a smishing kockázatai  |
| **Az esettanulmány leírása:** | Amint azt a "Kiberbiztonság otthon és az irodában" című modulból már tudja, az adathalászat a leggyakoribb támadás az európai KKV-k ellen, és ezek a támadások a támadáshoz használt módszertől függően változhatnak. Ebben az esettanulmányban a "smishingre", az SMS-en keresztül történő adathalászat technikájára összpontosítunk.Ez az esettanulmány a spanyolországi Nemzeti Kiberbiztonsági Intézettől (INCIBE) származik, amely a kiberbiztonsággal kapcsolatos valós történetek sorát közli, hogy felhívja a vállalatok figyelmét a szükséges vészhelyzeti intézkedések meglétének fontosságára.**Mi történt?**Egy KKV adminisztrációs osztályának egyik alkalmazottja volt felelős a vállalat csomagjainak fogadásáért és küldéséért különböző futárcégek szolgáltatásain keresztül. A vállalatnál naponta küldtek és fogadtak csomagokat, így ez a munkavállaló a termelési részlegnek szánt anyagokat tartalmazó dobozra várt.Aznap a munkavállaló SMS-t kapott a vállalati okostelefonjára egy látszólag csomagküldő cégtől. Az SMS jelezte, hogy az üzenetben megadott linken keresztül le kell tölteni egy alkalmazást a kézbesítés kezeléséhez, így a munkavállaló ezt meg is tette.Napokkal később a számlák kifizetéséért felelős kollégák figyelmeztették a munkavállalót, hogy a vállalati telefonszámlája sokkal magasabb a szokásosnál. Ennek oka az volt, hogy a készülékről a munkavállaló tudta nélkül rengeteg SMS-üzenetet küldtek a hónap folyamán.**Miért történt mindez?**Az alkalmazott "smishing" áldozata lett. Az SMS egy hamis feladótól érkezett, és a linkre kattintva és az alkalmazást letöltve megfertőzte a telefonját a "FluBot" vírussal, egy trójai programmal, amely azzal a céllal telepíti magát az androidos készülékekre, hogy banki adatokat lopjon el, és csomagküldő cégnek adva ki magát, azonnali cselekvésre szólítva fel a csomag elvesztésének elkerülése érdekében. Ezen túlmenően a kártevő a telefon címjegyzékét használja arra, hogy további hamis SMS-eket küldjön és további eszközöket fertőzzön meg, távolról parancsokat hajt végre, és megakadályozza, hogy a felhasználó eltávolítsa az alkalmazást.**Hogyan lehetett volna ezt elkerülni?**Bár a vállalat informatikai részlege végül helyreállította a munkavállaló telefonját, mindez elkerülhető lett volna az alábbi intézkedésekkel:* Kiberbiztonsági irányelvek bevezetése a vállalaton belül a vállalati eszközök és telepített alkalmazások használatának ellenőrzése és korlátozása érdekében.
* Ismeretlen forrásból származó alkalmazások telepítésének mellőzése.
* Gyanakvás a linkeket vagy mellékleteket tartalmazó üzenetekkel szemben.
* Az operációs rendszer és a vírusirtó minden biztonsági frissítésének aktiválása és frissítése.
 |
| **Bővebb információ:**  | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms>  |
| **Az esettanulmány célcsoportja:**  |  [x] Mikro-, kis- és középvállalkozások (KKV-k)[x] KKV-k munkavállalói [ ] Az EU szakképzési ökoszisztémája [ ] Vállalkozásokat támogató szervezetek  |
| **ESCO kompetenciák és készségek** |
| * Transzverzális készségek és kompetenciák
* Szociális és érzelmi készségek
* Kritikai gondolkodás
* Analitikus gondolkodás
* Problémamegoldás
* Önmenedzselés
* Üzleti menedzsment
* Alkalmazkodóképesség
* Reziliencia
* Kreativitás
* Hálózatépítés
* Kezdeményezőkészség
* Rugalmasság
* Nyitottság
* A komplexitás megértése
* Együttműködés
* Empátia
* Innováció
* Vezetői képességek
* Képességek
* Technológiai készségek
* Termékmarketing
* Digitális marketing
* Digitális készségek
* Kommunikáció
* Együttműködés
* Érzelmi intelligencia
* Tudás
* Üzlet menedzsment
* Online tanulás és képzés
* Hirdetés
* Felhőalapú számítástechnika
* Big data
* E-kereskedelem
* Mesterséges intelligencia
* Dolgok Internete (IoT)
* Digitális írástudás
* Kiberbiztonság
* Adatbányászat és -elemzés
* Fenntarthatóság
* Jólét
* Éghajlatváltozás
* Közösségi média menedzsment

  |