**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:** | WannaCry: a frissítések fontossága |
| **Az esettanulmány leírása:** | Az Európai Unió Kiberbiztonsági Ügynöksége 2017 májusában számolt be az első olyan európai szintű kiberügyi együttműködésről, amelyben több tagállammal együtt dolgoztak az uniós szabványos működési eljárások alkalmazásával. Ezt az együttműködést azonban egy tömeges zsarolóvírus által generált bonyolult helyzet váltotta ki.  A RESTART képzés 3. modulja szerint a zsarolóprogram a rosszindulatú programok olyan veszélyes típusa, amely titkosítja a fájlokat az eszköz merevlemezén, és korlátozza a felhasználó hozzáférését, váltságdíjat követelve - általában kriptovalutában - a fájlok visszafejtéséért cserébe.  **Mi történt?**  2017. május 12-én olyan esemény történt, amely világszerte több ezer számítógépet érintett: a "WannaCry" zsarolóvírus-támadás. Csak a támadás első néhány órájában 150 országban több mint 190 000 számítógépet érintett, köztük olyan kulcsfontosságú ágazatokat és szereplőket, mint az egészségügy, a közlekedés, az oktatás, az energia, a pénzügy és a távközlés és több uniós ország gyártóüzemének teljes gyártósorai is károsodtak.  Ez azután történt, hogy a számítógépük képernyőjén megjelent egy üzenet, amely szerint rendszereik és fájljaik a váltságdíj kifizetéséig zárolva lesznek.  **Miért történet ez?**  A WannaCry a Microsoft Windows operációs rendszer eszközeit érintette az MS17-010 sebezhetőség kihasználásával a hackerek által használt "EternalBlue" kódon keresztül.  Bár a zsarolóvírusok általában felhasználói interakciót igényelnek, például egy fertőzött e-mail melléklet letöltését vagy egy olyan weboldal meglátogatását, amely rosszindulatú programot tölt le az eszközre, a WannaCry esetében a fertőzéshez az eszköznek csak a Windows sebezhető verziójával kellett rendelkeznie.  A terjedés nagyon gyors volt, mivel az "SMBv1" nevű protokollt használta, amely az azonos hálózathoz csatlakoztatott nyomtatókkal és eszközökkel kommunikált a fertőzés folytatásához, és főként a fájlokat tette hozzáférhetetlenné és blokkolta a számítógépes programokat, váltságdíjat követelve a normális tevékenység helyreállításáért cserébe.  **Hogyan lehetett volna ezt elkerülni?**  Ma már tudjuk, hogy amikor mindez történt, a Windowsnak már volt egy frissített verziója, amely kijavította a Wannacry által kihasznált sebezhetőséget. Ezért a legegyszerűbben úgy lehetett volna elkerülni, ha a legfrissebb biztonsági frissítésekkel és frissített vírusirtóval rendelkezett volna. Emellett más intézkedések is segítenek abban, hogy a hatás kisebb legyen, vagy ne legyen:   * Rendszeres biztonsági mentés minden fájlról. * Kiberbiztonsági tudatossági kampányok lefolytatása az alkalmazottakkal. * Fertőzés esetén ne fizesse ki a váltságdíjat, hanem forduljon szakértői segítséghez, mivel a fizetés nem garantálja, hogy a felhasználók újra hozzáférhetnek a fájljaikhoz. |
| **Bővebb információ:** | <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> |
| **Az esettanulmány célcsoportja:** | Mikro-, kis- és középvállalkozások (KKV-k)  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 | |