**RESTART: Osposobljavanje poduzetnika u svrhu otpornosti i razvoja**

**Obrazac studije slučaja**

**(Rezultat 3 - Zadatak 3.1. & Zadatak 3.2)**

|  |  |
| --- | --- |
| **Autor studije slučaja:** | Internet Web Solutions |
| **Naziv modula kojemu studija slučaja pripada** | Modul 3: Kibernetička sigurnost u (kućnom) uredu |
| **Naslov studije slučaja:** | WannaCry: važnost ažuriranja |
| **Opis studije slučaja:** | Agencija Europske unije za kibernetičku sigurnost izvijestila je u svibnju 2017. o prvom slučaju kibernetičke suradnje na europskoj razini; radili su s nekoliko država članica koristeći Standardne operativne procedure EU. Međutim, ova je suradnja bila potaknuta kompliciranom situacijom koju je generirao masivni ransomware.  Prema RESTART edukacijama, ransomware je opasna vrsta zlonamjernog softvera koji šifrira datoteke na tvrdom disku uređaja i korisniku ograničava pristup te zahtijeva otkupninu, obično u kriptovalutama, u zamjenu za dekriptiranje datoteka.  **Što se dogodilo?**  U petak, 12. svibnja 2017. dogodio se događaj koji je utjecao na tisuće računala diljem svijeta: napad ransomwarea "WannaCry". Samo u prvih nekoliko sati napada bilo je pogođeno više od 190.000 računala u 150 zemalja, uključujući kritične infrastrukturne sektore i operatere kao što su zdravstvo, promet, obrazovanje, energetika, financije i telekomunikacije, a bile su pogođene i cijele proizvodne linije proizvodnih pogona zemalja EU.  Do toga je došlo nakon što se na zaslonima njihovih računala pojavila poruka da će njihovi sustavi i datoteke biti zaključani dok se ne plati otkupnina.  **Zašto se to dogodilo?**  WannaCry je utjecao na uređaje s operativnim sustavom Microsoft Windows iskorištavanjem ranjivosti MS17-010 kroz kod "EternalBlue" koji su koristili hakeri.  Iako ransomware obično zahtijeva interakciju korisnika s nečim, poput preuzimanja zaraženog e-mail privitka ili posjete web stranici koja preuzima zlonamjerni softver na uređaj, uvjet WannaCry-a bio je samo da uređaj ima ranjivu verziju sustava Windows.  Širenje je bilo vrlo brzo jer je koristio protokol nazvan "SMBv1" koji je komunicirao s pisačima i uređajima spojenim na istu mrežu kako bi nastavio sa zarazom, a uglavnom je činio datoteke nedostupnima i blokirao računalne programe, tražeći otkupninu u zamjenu za oporavak normalne aktivnosti.  **Kako se to moglo izbjeći?**  Danas znamo da je, kada se sve ovo dogodilo, Windows već imao ažuriranu verziju koja je popravila ranjivost koju je WannaCry iskorištavao. Zato bi najlakši način da se to izbjegne bio imati najnovija sigurnosna ažuriranja i ažurirani antivirusni program. Osim toga, druge mjere također pomažu da učinak malwarea bude manji ili nepostojeći jesu:   * Redovito sigurnosno kopiranje svih datoteka. * Provođenje kampanja podizanja svijesti zaposlenika o kibernetičkoj sigurnosti. * U slučaju zaraze nemojte plaćati otkupninu, nego kontaktirajte stručnu pomoć jer uplata ne jamči da će korisnici ponovno moći pristupiti svojim datotekama. |
| **Poveznica za više informacija:** | <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> |
| **Ciljana skupina studije slučaja:** | Mikro, mala i srednja poduzeća (MMSP)  Zaposlenici MMSP-a  EU VET ekosustav  Organizacije za poslovnu podršku |
| **ESCO kompetencije i vještine:** | |
| [molimo da istaknete kompetencije i vještine koje su usklađene s definicijama ESCO-a i koje razvija svaki dio ovog modula]   * Transverzalne vještine i kompetencije   + Društvene i emocionalne vještine   + Kritičko mišljenje   + Analitičko mišljenje   + Rješavanje problema   + Samoupravljanje   + Poslovno upravljanje   + Prilagodljivost   + Otpornost   + Kreativnost   + Umrežavanje   + Inicijativa   + Fleksibilnost   + Otvorenost   + Rješavanje složenih problema   + Suradnja   + Empatija   + Inovacija   + Vodstvo      * Vještine   + Tehnološke vještine   + Marketing proizvoda   + Digitalni marketing   + Digitalne vještine   + Komunikacija   + Suradnja   + Emocionalna inteligencija      * Znanja   + Poslovno upravljanje   + Online učenje i obuka   + Oglašavanje   + Računarstvo u Oblaku   + Veliki podaci   + E-trgovina   + Umjetna inteligencija   + IoT (Internet of Things – “internet stvari”)   + Digitalna pismenost   + Kibernetička sigurnost   + Rudarenje i analiza podataka   + Održivost   + Dobrobit   + Klimatske promjene   + Upravljanje društvenim mrežama | |