**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:** | Phishing + SMS: rizici smishinga |
| **Opis studije slučaja:** | Kao što već znate iz modula “Kibernetička sigurnost u (kućnom) uredu”, phishing je najčešći napad na europska mala i srednja poduzeća, a može varirati ovisno o metodi koja se koristi za napad. U ovoj studiji slučaja fokusiramo se na smishing, tehniku krađe identiteta putem SMS-a.  Ova studija slučaja izvučena je iz Nacionalnog instituta za kibernetičku sigurnost u Španjolskoj (INCIBE), koji tvrtkama pruža niz stvarnih priča povezanih s kibernetičkom sigurnošću kao mjeru za podizanje svijesti o važnosti uvođenja potrebnih mjera za nepredviđene situacije.  **Što se dogodilo?**  Zaposlenik u administrativnom odjelu malog i srednjeg poduzeća bio je zadužen za upravljanje prijemom i slanje paketa tvrtke putem usluga različitih kurirskih službi. Svakodnevno su se slale i primale pošiljke u poduzeću, pa je djelatnik čekao kutiju s materijalom za proizvodni odjel.  Tog je dana zaposlenik primio SMS na svoj korporativni pametni telefon od navodne službe za dostavu paketa. U SMS-u je bilo naznačeno da je potrebno preuzeti aplikaciju putem linka navedenog u poruci kako bi se izvršila isporuka, pa je djelatnik to i učinio  Nekoliko dana kasnije, kolege zaduženi za plaćanje računa upozorili su zaposlenika da je njegov poslovni telefonski račun mnogo veći nego inače. To se dogodilo zato što je ogroman broj SMS poruka poslan s uređaja tijekom mjeseca bez znanja zaposlenika.  **Zašto se to dogodilo?**  Zaposlenik je bio žrtva smishinga. SMS je došao od lažnog pošiljatelja, a klikom na poveznicu i preuzimanjem aplikacije zarazio je svoj telefon malwareom "FluBot", trojancem koji se instalira na Android uređaje s ciljem krađe bankovnih podataka predstavljajući se kao tvrtka za dostavu paketa koja vas poziva da odmah poduzmete mjere kako biste izbjegli gubitak paketa. Osim toga, zlonamjerni softver koristi imenik telefona za slanje više lažnih SMS poruka kako bi zarazio više uređaja, daljinski izvršava naredbe i sprječava korisnika da deinstalira aplikaciju.  **Kako se to moglo izbjeći?**  Iako je IT odjel tvrtke na kraju oporavio telefon, sve se to moglo izbjeći mjerama kao što su:   * Implementacija politika kibernetičke sigurnosti u tvrtke kako bi se kontrolirala i ograničila upotreba korporativnih uređaja i instaliranih aplikacija. * Izbjegavanje instaliranja aplikacija iz nepoznatih izvora. * Sumnjičavost prema porukama koje sadrže poveznice ili privitke. * Aktiviranje svih sigurnosnih ažuriranja operativnog sustava i antivirusa. |
| **Poveznica za više informacija:** | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms> |
| **Ciljana skupina studije slučaja:** | Mikro, mala i srednja poduzeća (MMSP)  Zaposlenici MMSP-a  EU VET ekosustav  Organizacije za poslovnu podršku |
| **ESCO kompetencije i vještine:** | |
| * 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 | |