**RESTART: Odolnosť a tréning pre MSP**

**Prípadová štúdia**

**(Projektový výsledok 3 - Úloha 3.1. & Úloha 3.2)**

|  |  |
| --- | --- |
| **Autor:** | Internet Web Solutions |
| **Názov modulu ku ktorému sa prípadová štúdia viaže:** | Modul 3: Kybernetická bezpečnosť v (home) office |
| **Názov prípadovej štúdie:** | Phishing + SMS: riziká smishingu |
| **Prípadová štúdia:** | Ako už viete z modulu "Kybernetická bezpečnosť v (home) office", najčastejším útokom na európske MSP je phishing, ktorý sa môže líšiť v závislosti od metódy použitej na útok. V tejto prípadovej štúdii sa zameriame na smishing, techniku phishingu prostredníctvom SMS.  Táto prípadová štúdia bola prevzatá z Národného inštitútu pre kybernetickú bezpečnosť v Španielsku (INCIBE), ktorý poskytuje sériu skutočných príbehov súvisiacich s kybernetickou bezpečnosťou ako opatrenie na zvýšenie povedomia spoločností o dôležitosti zavedenia potrebných núdzových opatrení.  **Čo sa vlastne stalo?**  Zamestnanec administratívneho oddelenia malého a stredného podniku bol zodpovedný za riadenie prijímania a odosielania zásielok spoločnosti prostredníctvom služieb rôznych kuriérskych spoločností. Denne sa v spoločnosti odosielali a prijímali balíky, takže tento zamestnanec čakal na škatuľu s materiálom pre výrobné oddelenie.  V ten deň dostal zamestnanec na svoj firemný smartfón SMS správu od spoločnosti, ktorá sa javila ako doručovateľ balíkov. V SMS správe sa uvádzalo, že na správu doručovania zásielok je potrebné stiahnuť aplikáciu prostredníctvom odkazu uvedeného v správe, a tak zamestnanec pristúpil k jej stiahnutiu.  O niekoľko dní neskôr kolegovia zodpovední za platby účtov upozornili zamestnanca, že jeho firemný účet za telefón je oveľa vyšší ako zvyčajne. Dôvodom bolo obrovské množstvo SMS správ, ktoré boli zo zariadenia odoslané v priebehu mesiaca bez vedomia zamestnanca.  **Prečo sa to stalo?**  Zamestnanec sa stal obeťou smishingu. SMS prišla od falošného odosielateľa a kliknutím na odkaz a stiahnutím aplikácie infikoval svoj telefón malvérom "FluBot", trojským koňom, ktorý sa inštaluje do zariadení so systémom Android s cieľom ukradnúť bankové informácie tým, že sa vydáva za spoločnosť doručujúcu balíky a vyzýva vás, aby ste okamžite podnikli kroky, ktoré zabránia strate balíka. Okrem toho malvér využíva adresár telefónu na odosielanie ďalších falošných správ SMS a infikovanie ďalších zariadení, na diaľku vykonáva príkazy a bráni používateľovi odinštalovať aplikáciu.  **Ako sa tomu dalo predísť?**  Hoci IT oddelenie spoločnosti nakoniec telefón zamestnanca obnovilo, všetkému sa dalo predísť takýmito opatreniami:   * Zavedenie zásad kybernetickej bezpečnosti v spoločnosti na kontrolu a obmedzenie používania podnikových zariadení a nainštalovaných aplikácií. * Neinštalovať aplikácie z neznámych zdrojov. * Byť podozrievavý voči správam, ktoré obsahujú odkazy alebo prílohy. * Mať aktivované a aktualizované všetky bezpečnostné aktualizácie operačného systému a antivírusového programu. |
| **Odkaz :** | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms> |
| **Cieľové skupiny:** | Mikro, malý alebo stredný podnikateľ  Zamestnanec v mikro, malom alebo strednom podniku  Poskytovateľ VET  Organizácia na podporu podnikania |
| **ESCO kompetencie a zručnosti** | |
| * Prierezové zručnosti a kompetencie * Sociálne a emočné zručnosti * Kritické myslenie * Analytické myslenie * Riešenie problémov * Manažment seba samého * Podnikový manažment * Adaptabilita * Odolnosť * Kreativita * Networking * Iniciatíva * Flexibilita * Otvorenosť * Pochopenie komplexnosti * Spolupráca * Empatia * Inovácie * Vodcovstvo / Leadership      * Zručnosti * Technologické zručnosti * Marketing produktu * Digitálny marketing * Digitálne zručnosti * Komunikácia * Spolupráca * Emocionálna inteligencia      * Znalosti * Podnikový manažment * Online vzdelávanie * Reklama * Cloud computing * Big dáta * E-commerce * Umelá inteligencia * IoT (Internet vecí) * Digitálna gramotnosť * Kybernetická bezpečnosť * Data mining a dátové analýzy * Udržateľnosť * Well-being * Klimatická zmena * Riadenie sociálnych médií | |