MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Jún 2022

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci jún riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily.

Špeciálnym typom incidentu spojeného s phishingom bol hlásený prípad úniku pracovnej e-mailovej komunikácie, ktorej preposielanie si útočník nastavil do svojej e-mailovej schránky v službe Gmail. Organizácia únik zistila až po trištvrte roku, keď sa na mailserver vrátila spätná odpoveď, že útočníkovo konto na Gmaili už neexistuje. Predpokladaný vektor získania prístupu do konta zamestnanca sú phishingom získané prihlasovacie údaje.

Ďalší incident spojený s únikom údajov vznikol z nedbalosti zamestnanca, ktorý odhadol kolegovu e-mailovú adresu v službe Gmail na základe jeho mena a bez jej overenia viacerí zamestnanci na ňu posielali pracovné dáta. Majiteľom schránky sa ukázala byť zahraničná fyzická osoba, ktorá na problém opakovane bezúspešne upozorňovala. Podstata problému, ktorý viedol k incidentu, neleží iba v popísanej nedbalosti zamestnancov. Je ňou tiež samotné preposielanie pracovnej komunikácie a dát na súkromné e-mailové účty, resp. účty vo voľne dostupných webmailových službách.

Jednotka CSIRT.SK vykonávala tiež analýzy malvéru prítomného v prílohách škodlivých e-mailových správ a komunikovala s niekoľkými organizáciami v jej konštituencii ohľadom odstraňovania zraniteľností odhalených v ich IT infraštruktúre.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK informovala organizácie vo svojej správe o masívnej phishingovej kampani smerujúcej na subjekty v SR a indikátoroch kompromitácie s ňou spojených. CSIRT.SK ďalej vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje.

Mesačník zraniteľností Jún 2022

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné závažné zraniteľnosti
    - Microsoft Office: Follinna

https://www.csirt.gov.sk/posts/2908.html?csrt=2882614898807275317