MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Júl 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 júl riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytlo sa viacero prípadov rozposielania phishingu z kompromitovaných e-mailových kont niekoľkých organizácií. Pri jednej organizácii sa vyskytli kompromitované kontá opakovane. Všetky prípade boli pravdepodobne spojené s úspešnými útokmi s použitím sociálneho inžinierstva (phishingu) na zamestnancov. Pri preverovaní administrátori neodhalili stopy kompromitácie mailserverov.

Významnejším incidentom v mesiaci júl bol ransomvérový útok na obecný úrad. Obec stratila údaje o mzdách, evidenciu obyvateľstva a majetku a iné. CSIRT.SK sa podarilo obnoviť väčšinu dát zo shadow copies, ktoré neboli zašifrované.

Jednotka CSIRT.SK komunikovala s niekoľkými organizáciami v jej konštituencii ohľadom odstraňovania zraniteľností odhalených v ich IT infraštruktúre.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK 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 Júl 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
    - Atlassian

https://www.csirt.gov.sk/posts/2947.html?csrt=500713598601953054