

# Riziká nahrávania citlivých údajov do verejných online služieb

CSIRT.SK upozorňuje organizácie a jednotlivcov na riziká spojené s nahrávaním citlivých alebo interných údajov do verejne dostupných externých platforiem. Mnohé z nich spracúvajú používateľské dáta mimo kontrolovaného prostredia organizácie, čo môže predstavovať významné bezpečnostné riziko. Tieto služby sú často využívané na analýzu škodlivého softvéru, phishingových kampaní alebo podozrivých súborov, pričom umožňujú interaktívne spracovanie nahraných dát v cloudovom prostredí.



## Aké údaje bývajú najčastejšie zdieľané?

V praxi dochádza k situáciám, keď používatelia nahrávajú do verejných analytických platforiem:

- celé e-mailové správy vo formáte .eml alebo .msg,
- e-mailové hlavičky obsahujúce interné smerovanie a infraštruktúru,
- prílohy z reálnej firemnej komunikácie,
- URL adresy z aktívnych kampaní,
- dokumenty obsahujúce interné alebo osobné údaje,
- konfiguračné a diagnostické súbory zo systémov.

## Hlavné riziká

Nevhodné používanie externých online služieb môže viesť k:

- úniku citlivých informácií z e-mailovej komunikácie,
- zverejneniu interných technických detailov (domény, IP adresy, infraštruktúra),
- kompromitácii prebiehajúcich incidentov alebo vyšetrovaní,
- porušeniu GDPR a interných bezpečnostných politík,
- neúmyselnému zdieľaniu dôverných obchodných informácií.

Zvlášť rizikové je nahrávanie reálnych e-mailových konverzácií, ktoré môžu obsahovať identifikátory zamestnancov, klientov alebo interných procesov.

## Odporúčanie

Rastúce využívanie externých online služieb prináša organizáciám nové možnosti, ale aj nové riziká. Nesprávne zaobchádzanie s citlivými údajmi môže mať závažné bezpečnostné, právne aj reputačné dôsledky. CSIRT.SK preto odporúča organizáciám venovať zvýšenú pozornosť kontrole údajov odosielaných do externých služieb a dôsledne uplatňovať princíp minimalizácie dát a bezpečnostné pravidlá pri práci s citlivými informáciami.