Korešpondenčná adresa :

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR,
Sekcia kybernetickej bezpečnosti,
a VJ CSIRT
Pribinova 25
811 09 Bratislava

Sídlo pobočky VJ CSIRT Bratislava
Tower 115, Pribinova 25, 811 09 Bratislava

Sídlo pobočky VJ CSIRT Košice
(oddelenie Analýzy kybernetických hrozieb)
Boženy Němcovej 5, 040 01 Košice

Kontakt pre hlásenie incidentov:

incident@csirt.sk
+421 948 039 525

Súrne prípady mimo pracovných hodín:
+421 940 504 241
+421 940 504 227
+421 948 936 766

incident@csirt.sk
+421 948 039 525

Centrálny portál kybernetickej bezpečnosti

CSIRT.SK

LETÁK PRVEJ POMOCI

KYBERNETICKÝCH INCIDENTOV

LEPŠIE BYŤ PRIPRAVENÝ,
AKO PREKVAPENÝ

Spolufinancovaný Európskou úniou
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

O NÁS

Sekcia kybernetickej bezpečnosti prostredníctvom VJ CSIRT, poskytuje služby verejnej správe za účelom reakcie na bezpečnostné incidenty namierené na Informačné technológie verejnej správy (ITVS).

Postup nahlasovania incidentov

1. Príprava informácií (obsah e-mailu)

Pred nahlásením incidentu je dôležité zhromaždiť čo najviac relevantných informácií. Tieto informácie môžu zahŕňať:

- **Popis incidentu:** Detailný popis toho, čo sa stalo, vrátane času a spôsobu zistenia.
- **Zasiahnuté zariadenia:** Typ a funkcia zariadenia, IP adresa, hostname, operačný systém a zasiahnutý softvér.
- **Protiopatrenia:** Aké opatrenia boli vykonané na zmiernenie incidentu.
- **Kontaktné údaje:** Informácie o osobe, ktorá incident nahlasuje, vrátane funkcie a názvu organizácie.

2. Nahlásenie incidentu

Incident je možné nahlásiť nasledujúcimi spôsobmi:

E-mailom:

- VJ CSIRT: **incident@csirt.sk**.
  K e-mailu je možné priložiť prílohy a v prípade potreby využiť aj PGP kľúč na ich zašifrovanie.

Telefonicky:

- **V prípade urgentných incidentov** je možné kontaktovať CSIRT **telefonicky**
  +421 948 039 525

- Súrne prípady **mimo pracovných hodín:**
  +421 940 504 241
  +421 940 504 227
  +421 948 936 766

3. Po nahlásení

Po nahlásení incidentu tím VJ CSIRT analyzuje poskytnuté informácie a podnikne potrebné kroky na zmiernenie alebo odstránenie hrozby. Môže vás kontaktovať pre ďalšie informácie alebo poskytnúť odporúčania na ďalšie kroky. Okrem zákonnej povinnosti nahlásiť kybernetický incident NBÚ na SK-CERT, je nevyhnutné tento incident nahlásiť aj na CSIRT.

TYPY INCIDENTOV

- **Nežiaduci obsah** - spam, obťažovanie
- **Škodlivý kód** - vírus, červ, trójsky kôň, spyware, dialler
- **Získavanie informácií** - skenovanie, odpočúvanie, sociálne inžinierstvo
- **Pokus o prienik** - využitie známej zraniteľnosti, opakované pokusy o prihlásenie, útok s neznámymi znakmi
- **Prienik** - skompromitovanie privilegovaného účtu, skompromitovanie obmedzeného účtu, skompromitovanie aplikácie, botnet
- **Nedostupnosť** - DoS, DDoS, sabotáž
- **Ohrozenie bezpečnosti informácií** - neoprávnený prístup k informáciám, neoprávnená zmena informácií
- **Podvod, sprenevera** - neoprávnené využívanie zdrojov, porušenie autorských práv, prevzatie identity, phishing