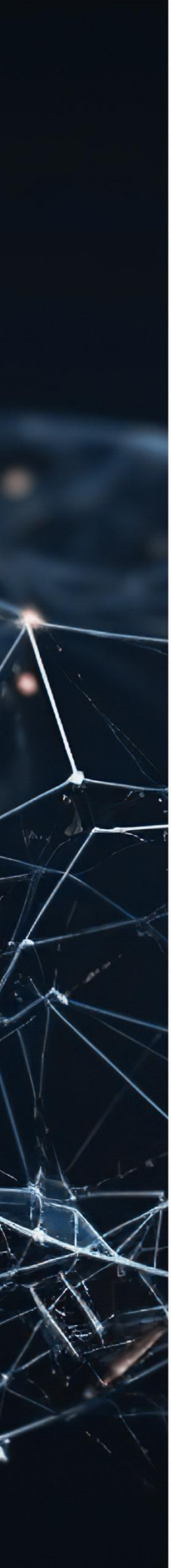


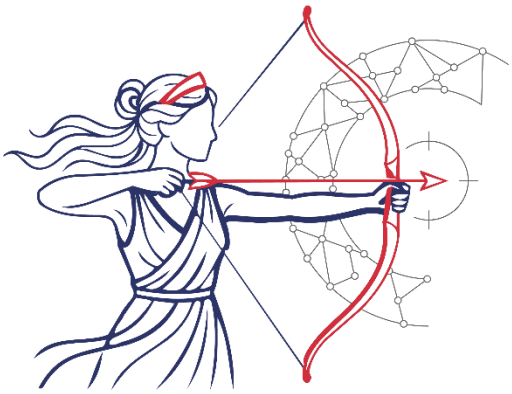
MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie o

REAKTÍVNYCH SLUŽBÁCH

VJ CSIRT



REAKTÍVNE
ČINNOSTI

Reaktívne služby VJ CSIRT

Vládna jednotka CSIRT pôsobí ako národný odborný garant pre oblasť informačných technológií verejnej správy. Jej cieľom je zabezpečovať kybernetickú odolnosť štátu poskytovaním dvoch hlavných kategórií služieb - **reaktívne služby** a **proaktívne služby**. Primárne služby VJ CSIRT sú služby reaktívne.

Reaktívne služby sa zameriavajú na priamu pomoc pri riešení už vzniknutých incidentov, ich triáž, analýzu škodlivého kódu a digitálnu forenznú analýzu s cieľom minimalizovať dopady útokov.

Koordinácia pri riešení incidentov a podpora krízového manažmentu: Táto služba zahŕňa komunikáciu s dotknutými subjektmi v podobe metodickej a technickej pomoci, koordináciu spoločného postupu, distribúciu upozornení, koordináciu aktivít medzi jednotlivými zložkami, pravidelné hlásenie stavu riešenia incidentu a poskytovanie odporúčaní na okamžité opatrenia na zamedzenie ďalšieho šírenia útoku.

Služby poskytované oddelením L1

Naše služby oddelenia L1 sa delia na 2 časti: primárna (spojená s riešením incidentu) a sekundárna (aktivity vykonávané mimo aktívny incident).

1. **Primárna činnosť:** ide o poskytovanie súčinnosti pri riešení incidentov subjektov verejnej správy. Jedná sa o prvotné zaistenie dát, ich vyhodnotenie a koordinácia ďalej vykonaných krokov. L1 zároveň poskytuje súčinnosť pri riešení incidentov v konštituencii „nadriadených“ organizácií (napr. NBÚ, CKO a pod.). V rámci riešenia incidentov je nutné poskytovať aj koordinačnú činnosť pre korektnú reakciu na vzniknutý incident, ako aj návrh opatrení pre ich mitigáciu a zníženie rizika ich opätovného vzniku v budúcnosti. Na základe analýzy a navrhnutých krokov L1

rozdeľuje a koordinuje kroky pre špecifikované oddelenia riešenia KBI. Postup riešenia incidentu je možné nájsť nižšie, viď. Obr. 1.

Obrázok 1 Postup riešenia incidentu

2. **Sekundárna činnosť:** činnosti mimo riešenia aktívneho incidentu sú predovšetkým spojené s proaktívnym rozširovaním povedomia, spoluprácou s inými CSIRT jednotkami na ladení nových nástrojov a procedúr, ako aj vytváranie, implementácia, manažment a dokumentácia vlastných aplikácií a technických riešení. Zároveň sa oddelenie L1 účastní na praktických cvičeniach a konferenciách za účelom rozšírenia znalostí, kontaktov a ďalších možností fungovania.

Nahlasovanie kybernetického bezpečnostného incidentu (KBI) Vládnej jednotke CSIRT.SK

1. Kam a ako zaslať hlásenie

- Hlásenie sa zasiela **e-mailom** na adresu **incident@csirt.sk.**
    - Komunikovať je možné aj telefonicky na kontakty uvedené na **webe** v časti *„Kontakt pre hlásenie incidentov“* (takáto komunikácia neplní účel riadneho nahlásenia incidentu a slúži iba na účely konzultácie, resp. vysvetlenie prípadných nejasností alebo dodatočných otázok)

- Šifrovanie: V prípade potreby je možné na zašifrovanie príloh **využiť PGP kľúč** (voľne dostupný napr. cez nástroj **GNU GPG).** Kľúč VJ CSIRT je možné nájsť na **webe** v časti *„PGP kľúč na bezpečnú komunikáciu“.*
- Identifikácia: Je nutné uvádzať korektnú e-mailovú adresu, ktorá bude slúžiť ako primárny kontakt pre ďalšiu komunikáciu.

2. Čo musí hlásenie obsahovať

Pri popise incidentu je dôležité uviesť čo najviac informácií pre rýchlu analýzu. Medzi kľúčové údaje patria:

A. Informácie o ohlasovateľovi:

- Pracovné zaradenie a funkcia osoby, ktorá incident hlási.
- Názov a typ organizácie (štátna, súkromná, škola a pod.).
- Ďalšie dotknuté organizácie.

B. Informácie o incidente:

- Časové údaje - kedy incident začal (ak je známy) a kedy/ako bol zistený.
- Boli zneužité nejaké známe zraniteľnosti? (áno/nie/neviem).
- Aktuálny stav - či ide o prebiehajúci incident a aké protiopatrenia už boli vykonané.
- Detailný popis - priebeh incidentu, použité typy útokov, smer útoku a informácia o tom, či boli prekonané bezpečnostné opatrenia (napr. firewall, antivírus).

C. Informácie o zasiahnutých zariadeniach:

- typ, funkcia, IP adresa a hostname zariadenia,
- operačný systém a zasiahnutý softvér,
- protokol a porty na ktoré útok smeroval,
- popis hardvéru zariadenia,

- zasiahnutý softvér alebo súbory,
- kontaktná osoba pre získanie prístupu k zariadeniu,
- informácia, či ide o kritické zariadenie pre kontinuitu činnosti a či obsahuje neverejné informácie.

- Kompletné informácie aj s pomôckami je možné nájsť na našom **webe** v časti *„Nahlásiť incident.“*

Zároveň je nutné dodať, že CSIRT.SK ako vládna jednotka pre riešenie počítačových bezpečnostných incidentov pomáha pri riešení kybernetických bezpečnostných incidentov ***organizáciám štátnej a verejnej správy, konkrétne pre oblasť informačných technológií verejnej správy*** *(úlohy v oblasti prevencie a riešenia kybernetických bezpečnostných incidentov upravuje zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe - upravuje správu IT vo verejnej správe a definuje povinnosti orgánov riadenia v oblasti bezpečnosti, v rámci čoho VJ CSIRT plní úlohy pri nepretržitom monitorovaní informačných technológií verejnej správy, hodnotení zraniteľností).*

3. Pravidlá pre špecifické typy incidentov

Podľa **typu hrozby** by mal e-mail obsahovať aj tieto informácie:

- Vírus/Malvér - dotknutý súbor zašlite zabalený v archíve ZIP so stanoveným heslom: „incident“.
- Spam - pripojte úplnú hlavičku aj telo e-mailovej správy.
- Phishing: Uveďte úplnú adresu URL.
- DoS útok/Sieťové skenovanie: Priložte časové známky, zdrojové a cieľové IP adresy, porty a ideálne aj vzorku zachytených paketov (napr. z programu WireShark).

4. Spracovanie hlásenia

Hlásenie prijaté e-mailom spracováva **L1 tím (prvotný príjem a triáž)**. Ten incident posúdi a v prípade, že ide o incident vyžadujúci súčinnosť, aktivujú sa reaktívne služby (L1, L2 alebo L3 pomoc), koordinácia riešenia, prípadne forenzná či malvérová analýza.

Dôležité upozornenie: Pri získavaní informácií o incidente dbajte na to, aby **citlivé údaje** vašej organizácie neunikli **cez verejné webové služby.**

Čo služba poskytuje

VJ CSIRT poskytuje široké spektrum odborných činností:

- **Koordinácia a podpora:** Riadenie komunikácie a aktivít jednotlivých zložiek počas prebiehajúceho incidentu.
- **Technická pomoc (L1, L2, L3):** Hĺbková analýza incidentov, asistencia pri prvotnom zbere a analýze získaných dát, návrh ďalších postupov (forenzná analýza, mitigácia, obnova a pod.).
- **Technická analýza:** Analýza zasiahnutých staníc, serverov a sieťových dát s cieľom identifikovať spôsob napadnutia a možné dopady.
- **Zaisťovanie dát:** Podpora pri vytváraní kópií diskov, obrazov pamäte a extrakcii logov potrebných pre ďalšie skúmanie.

Obmedzenia služby

- **Nenahrádza zodpovednosť správcu:** Poskytovanie služieb VJ CSIRT nezbavuje prevádzkovateľa základnej služby ani ústredný orgán ich zákonnej zodpovednosti za plnenie povinností v oblasti kybernetickej bezpečnosti.

- **Potreba súčinnosti:** Reaktívne služby sú vykonávané vždy za účasti prevádzkovateľa, ktorý o pomoc požiadal, jednotka nemôže incident riešiť izolovane bez súčinnosti dotknutého subjektu.
- **Ochrana národných záujmov:** Služba nesmie poskytovať informácie, ktorých zverejnenie by bolo v rozpore so základnými bezpečnostnými záujmami štátu.
- **Bežní občania a súkromný sektor:** VJ CSIRT bežne nerieši incidenty u bežných občanov ani v širšom súkromnom sektore.
- **Pracovný režim:** Väčšina odborných služieb (okrem monitoringu L1/L2) je štandardne poskytovaná v režime 8/5, čo znamená, že plná technická podpora nemusí byť okamžite dostupná mimo pracovných hodín, ak nejde o kritickú krízovú situáciu.

Často kladené otázky (FAQ)

1. Sme súkromná firma — môžeme kontaktovať VJ CSIRT?

VJ CSIRT poskytuje služby výhradne organizáciám štátnej a verejnej správy v oblasti IT VS. Súkromné subjekty môžu kontaktovať NBÚ prostredníctvom portálu **JISKB** alebo komerčné CSIRT/SOC tímy.

2. Bude VJ CSIRT automaticky informovať políciu?

Nie. VJ CSIRT neohlasuje incidenty orgánom činným v trestnom konaní bez súdneho príkazu alebo explicitnej žiadosti postihnutej organizácie. V prípade, ak Vám vznikla škoda, odporúčame Vám podať trestné oznámenie na najbližší útvar Policajného zboru, spolu so všetkými dôkaznými prostriedkami, ktoré máte k dispozícii, resp. zaslať Váš podnet na **incident@minv.sk.**

3. Sú informácie o incidente dôverné?

Áno. Všetky informácie sú spracovávané dôverne podľa **TLP protokolu.** Citlivé informácie sú zdieľané len na základe potreby vedieť (need-to-know) a anonymizovane.

4. Vznikol bezpečnostný incident. Čo treba robiť ?

V prípade vzniku bezpečnostného incidentu je potrebné vždy kontaktovať zodpovednú osobu v rámci organizácie v závislosti od interných predpisov a štandardov, ktorými sa daná organizácia riadi (správca IS, bezpečnostný manažér, a pod.). Následne je potrebné zabezpečiť prvotné úkony spojené s riešením vzniknutého incidentu, zdokumentovať všetky skutočnosti, ktoré by mohli napomôcť pri jeho riešení a vykonať potrebné kroky na odstránenie alebo zmiernenie jeho dopadov.

5. Čo mám urobiť pred tým, ako zavolám alebo napíšem?

Zaznamenajte čas zistenia incidentu, zachovajte logy a dôkazy, nevypínajte zasiahnuté zariadenia (odpojte ich od internetu), aktivujte vlastné interné protiopatrenia a pripravte zoznam zasiahnutých systémov. Čím viac informácií dokážete zistiť a uchovať, tým rýchlejšie dokážeme navrhnúť potrebné kroky. Potrebné informácie získate **tu.**