CSIRT.CZ
Riešenie bezpečnostných incidentov

Zuzana Duračinská • zuzana.duracinska@nic.cz •
23.11.2014

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC z.s.p.o.

- Záujmové združenie právnických osôb
- Správa registru doménových mien .CZ

*****1 225 193*****

- **https://www.nic.cz**
- **kontakt@nic.cz, +420 222 745 111**

CZ.NIC | AKADEMIE

CZ.NIC | LABS

SKENER WEBU

captchahelp

mojeID

Tablexia

CSIRT.CZ
powered by CZ.NIC

BIRD

JAK NA INTERNET

PROJECT:TURRIS

KNOT DNS

CZ.NIC | SPRÁVCE DOMÉNY CZ

CSIRT.CZ

- Computer Security Incident Response Team
- Plní rolu Národného CSIRT tímu Českej republiky podľa Zákona o kybernetickej bezpečnosti
- Medzinárodne uznaný tým organizáciami **FIRST** a **Trusted Introducer**
- Nemá výkonné právomoci

- **https://www.csirt.cz**
- **info@csirt.cz, +420 910 101 010**

CSIRT.CZ – cieľové skupiny

- Operátori
- IT odborníci
- Bezpečnostná (národná a medzinárodná) komunita
- Koncoví užívatelia

- Prijímanie hlásení o incidentoch a prijímanie kontaktných údajov
- Riešenie incidentov
- Budovanie spolupráce
- Proaktívna činnosť
- Vzdelávanie
- Informovanie o nákaze v doméne .CZ

Kedy sa incident hlási týmu CSIRT.CZ?

- **Zákonná** povinnosť - operátor patrí pod §3 písm.b) ZKB

  (orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d)

- Bezpečnostný incident **pretrváva**
- Nikto na hlásený incident **nereaguje** (v rámci ČR / mimo ČR)
- Na hlásený incident bola prijatá **odmietavá odpoveď**
- Nieje možné detekovať **zdroj útoku** (sieť/IP adresu)
- Problém by mohol byť **plošný**
- CSIRT.CZ ako **last resort!**

Ako incident nahlásiť?

- **Jednoduchý** a **zrozumiteľný** textový e-mail
- Správa by mala obsahovať **IP adresu (URL)** alebo **adresný blok**, ktorého sa to týka
- Typ incidentu (napr. spam, virus, DDOS, phishing, pharming...)
- Časť logu

  - časové známky a časová zóna

  - zdrojová a cieľová IP adresa

  - zdrojový a cieľový port

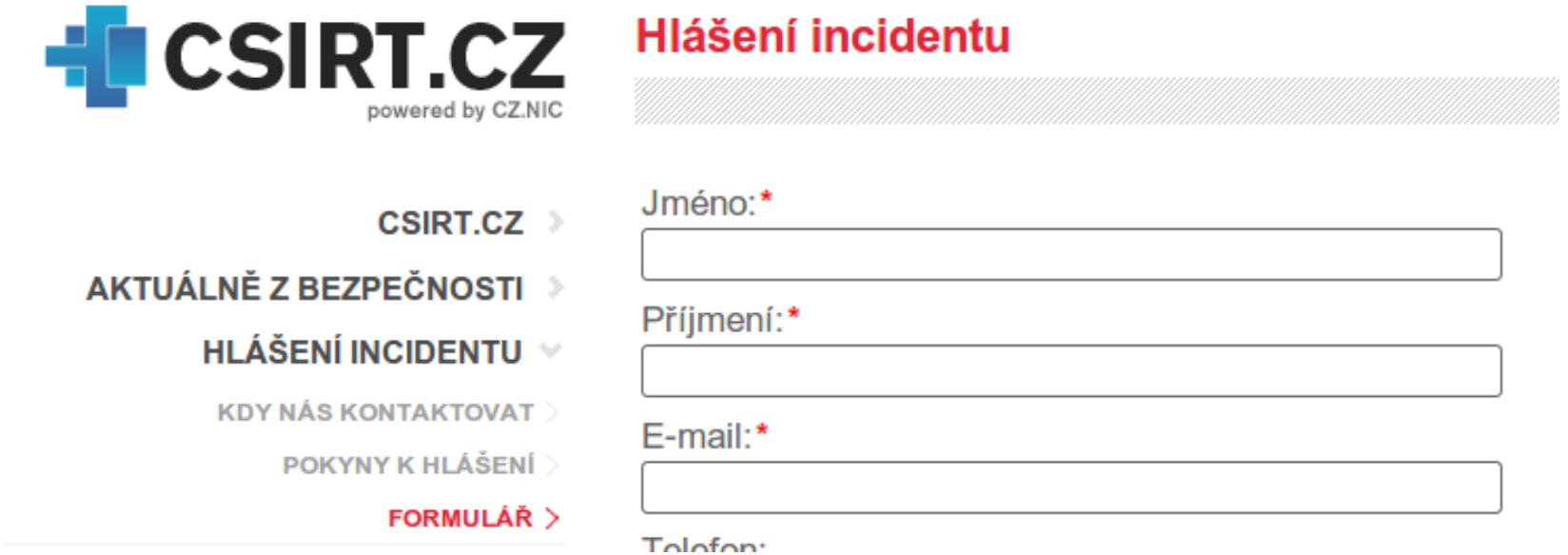
  - TCP-UDP-ICMP

- Adresa pre hlásenie: **abuse@csirt.cz**

Ako incident nahlásiť?

- Cez formulár na:

  https://csirt.cz/incidentreport/



Incident Handling

- Proces riešenia incidentov
- Niekoľko fázový proces
- Vyžaduje vysokú pružnosť riešenia
- Každý incident je posudzovaný individuálne
- Nutné ručné resp. poloautomatické riešenie
- Pre (spolu)riešenie incidentu viacerými stranami je nutná určitá dávka dôvery
- Všetky informácie a štatistiky sú z našej strany anonymizované

Čo nasleduje po nahlásení incidentu?

- Vykonáme prvotnú analýzu
- Zistíme, či máme dostatok informácií
- Kontaktujeme zdroj problému (držiteľ IP adresy, domény, web hosting, databáza TI, datábaza FIRST, znalosť infraštruktúry...)
- Skontrolujeme či sa problém medzičasom neodstránil (možné napr. u phishingu)
- Sprostredkujeme odpoveď

Čo nasleduje po nahlásení incidentu?

- Každý incident vyžaduje individuálne posúdenie
- Incidenty sa môžu opakovať
- Informujeme aj ďalšie potencionálne obete
- V prípade plošných incidentov vytvoríme informačný odkaz na webe, prípadne kontaktujeme média
- V prípade potreby vytvoríme návod na obranu

Rýchlosť vyriešenia incidentu

- Záleží od závažnosti incidentu a miere jeho sofistikovanosti
- Záleží od typu incidentu
- Záleží od schopností a vôle jednotlivých strán
- Čas na riešenie sa pohybuje od niekoľko minút po niekoľko týždňov

Nástroje na riešenie incidentov

- CERT/CSIRT týmy využívajú najčastejšie ticketovacie systémy RTIR alebo OTRS
- Open-source ticketovacie systémy pre riešenie incidentov
- Možné sledovanie cyklu incidentu
- Multi-user systémy
- Možnosť spájania ticketov
- Automatické vyplnenie informácií nevyhnutných pre riešenie incidentu (IP adresa, AS, kontakt...)

Ďakujem za pozornosť
Otázky?

Zuzana Duračinská • zuzana.duracinska@nic.cz