RFC2350 - Popis CSIRT společnosti DATASYS s. r. o., dále jen DATASYS

1. Informace o dokumentu

Tento dokument obsahuje informace, týkající se řešení skupinově významných incidentů v oblasti kybernetické bezpečnosti společnosti DATASYS.

Dokument je koncipován podle standardu RFC 2350 a poskytuje základní informace o DATASYS eSOC CSIRT, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

- **Název:** RFC 2350 Profil - DATASYS CSIRT
- **Verze:** 1.0
- **Datum vydání:** 13. 3. 2026
- **Platnost:** Do odvolání
- **Umístění:** https://www.datasys.cz/csirt/rfc2350.txt
- **Distribuční seznam pro oznámení**

  Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu esoc@datasys.cz.

2. Kontaktní informace

- **Název týmu:** DATASYS eSOC CSIRT
- **Adresa:** DATASYS s.r.o., Zengrova 85, 703 00 Ostrava – Vítkovice, Česká republika
- **Časové pásmo:** CET/CEST (GMT+1/+2)
- **Telefon:** +420 225 308 250 (mimo standardní pracovní dobu je toto telefonní číslo přesměrováno na pohotovost)
- **E-mail:** esoc@datasys.cz

  e-mailová adresa je určena pro veškerou komunikaci s DATASYS eSOC CSIRT včetně hlášení incidentů
- **Web:** https://www.datasys.cz/

- **Šifrování:** PGP klíč

  Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:
  Type: EdDSA/256 **Expires:** never
  Fpr: (Floating Point Regster) 3A6F C754 C25E 5DCB D126 8FBA C862 2DB3 040B 4C8E
  UID: esoc_datasys.cz esoc@datasys.cz

3. Informace o týmu

- **Odpovědnost:** DATASYS CSIRT zajišťuje bezpečnostní dohled pro interní infrastrukturu DATASYS a komerční SOC služby pro zákazníky.
- **Vedoucí týmu:** Eva Golombková, e-mail: golombkova@datasys.cz
- **Členové týmu:** kompletní přehled členů týmu týmu DATASYS eSOC CSIRT není veřejně k dispozici.
  Členové týmu se při oficiální komunikaci ohledně incidentu představí protistraně plným jménem.
- **Sponzor:** Vedení DATASYS s.r.o.
- **Pravomoc:** Tým má pravomoc přijímat opatření k izolaci ohrožených systémů v rámci sítě DATASYS a u zákazníků na základě SLA.
- **Další informace:** preferovaný způsob kontaktování DATASYS eSOC CSIRT je prostřednictvím e-mailu.
  Není-li možné (nebo není-li to z bezpečnostního hlediska vhodné) použít e-mail, můžete DATASYS eSOC CSIRT kontaktovat telefonicky na čísle uvedeném v **bodě 2. Kontaktní informace.**

- **Provozní doba eSOC CSIRT:** Standardní operace probíhají v pracovní dny **od 07:00 do 17:00 hod.** Monitoring, příjem hlášení a reakce na incidenty (on-call) jsou zajištěny v režimu **24/7**.

4. Charakteristika

- **Poslání:** Zajišťování kybernetické bezpečnosti, detekce a reakce na incidenty pro komerční zákazníky (eSOC) i pro interní potřeby společnosti.
- **Komunita (Constituency):** Interní infrastruktura DATASYS a zákazníci využívající komerční služby eSOC.

- **Autorita:** CSIRT operuje pod záštitou společnosti DATASYS s.r.o. a je držitelem certifikace Trusted Introducer.

5. Politiky

- **Typy incidentů:** Tým řeší pokusy o průnik, Malware, Ransomware, neoprávněný přístup, identifikace DoS útoků a další hrozby definované v SLA se zákazníky.
- **Spolupráce:** DATASYS spolupracuje s národním týmem CSIRT.CZ a mezinárodní komunitou v rámci akreditace.

  Dále je připraven spolupracovat s ostatními důvěryhodnými bezpečnostními týmy v ČR i zahraničí.
  S informacemi získanými v rámci činnosti DATASYS eSOC CSIRT, nebo sdílenými v rámci komunity bezpečnostních týmu bude nakládáno v souladu s požadavky české legislativy.
- **Sdílení informací:** Informace jsou sdíleny v souladu s TLP (Traffic Light Protocol).

6. Služby

Proaktivní služby:

- **Znalostní podpora:** Konzultace, řešení bezpečnostních problémů a asistence při konfiguraci bezpečnostních prvků.
- **Management zranitelností:** Na základě potřeb klienta provádíme skeny zranitelností a bezpečnostní audity, které umožňují proaktivní identifikaci slabých míst v infrastruktuře.
- **Threat Intelligence (CTI):** Vlastní analytická činnost v oblasti taktik, technik a postupů (TTPs) útočníků.

Reaktivní služby:

- **Detekce a analýza:** Primárním nástrojem je vlastní SIEM platforma ELISA, která zajišťuje sběr, integraci a analýzu logů ze síťových zařízení a dalších bezpečnostních nástrojů. Provádíme nepřetržitou detekci anomálií v chování sítě a vyhodnocování bezpečnostních událostí.
- **Reakce na incidenty:** Aktivace předem definované reakce při detekci hrozby. Službu jsme schopni provozovat i nad jinými SIEM nástroji a jinými bezpečnostními nástroji typu EDR, NDR atd. dle požadavků klienta.

7. Hlášení incidentů

- Incidenty hlašte e-mailem na **esoc@datasys.cz**. Uveďte co nejvíce podrobností (logy, čas, IP adresy).

8. Odmítnutí odpovědnosti

- DATASYS CSIRT nenese odpovědnost za přímé škody vzniklé v důsledku incidentu.

Eva Golombkova

Digitálně podepsal Eva Golombkova
Datum: 2026.03.13 09:07:35 +01'00'