SPRÁVA ŽELEZNIC

Veřejné

SŽ RFC 2350 STANDARD

POPIS TÝMU CSIRT SZ SPRÁVA ŽELEZNIC, S.O.

OBSAH

ZKRATKY A ZNAČKY

Níže uvedený seznam obsahuje zkratky a značky použité v tomto dokumentu. V seznamu se neuvádějí legislativní zkratky, zkratky a značky obecně známé, zavedené právními předpisy, uvedené v obrázcích, příkladech nebo tabulkách.

CERT.....Computer Emergency Response Team

CSIRT .....Computer Security Incident Response Team

FIRST.....Fórum CISRT týmů pro reakci na incidenty a bezpečnost

ID.....Identification

OJ.....Organizační jednotka

RFC.....Reguest For Comments

SELČ.....Středoevropský letní čas

SZT .....Správa železniční telematiky

TI .....Trusted Introducer

UTC .....Coordinated Universal Time

Kybernetický bezpečnostní incident..... Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Kybernetická bezpečnostní událost..... Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací

1 ÚVODNÍ USTANOVENÍ

1.1 Popis CSIRT SZ

Tento dokument obsahuje popis týmu CSIRT SZ Správa železnic, s.o., a to v souladu se standardem RFC 2350. Dokument poskytuje přehledným a strukturovaným způsobem základní informace o týmu CSIRT SZ, možnostech jeho kontaktování, odpovědnosti a poskytované služby.

1.2 Datum poslední aktualizace dokumentu

Toto je prvotní verze dokumentu s pořadovým číslem jedna, a to ze dne 22. srpna 2023

1.3 Distribuční seznam pro oznámení

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky zasílejte na e-mailovou adresu týmu CSIRT SZ, a to **soc@spravazeleznic.cz.**

1.4 Dostupnost dokumentu

Aktuální verze tohoto dokumentu naleznete vždy na:

https://www.spravazeleznic.cz/o-nas/kyberneticka-bezpecnost/csirt

2 KONTAKTNÍ INFORMACE

2.1 Název týmu

CSIRT SZ, tedy Computer Security Incident Response Team Správy železnic, s.o.

2.2 Adresa

CSIRT SZ
V Celnici 1028/10
110 00 Praha 1
Česká republika

2.3 Časové pásmo

Středoevropský čas (UTC +1, od poslední neděle v říjnu do poslední neděle v březnu) SELČ,
Středoevropský letní čas (UTC +2, od poslední neděle v březnu do poslední neděle v říjnu).

2.4 Telefonní číslo

+420 **972 235 333** (linka je dostupná 24/7/365).

2.5 Ostatní telekomunikace

Žádné.

2.6 Elektronická adresa

Oznámení (hlášení) incidentu zasílejte na e-mailovou adresu **soc@spravazeleznic.cz**. Na obdržený e-mail je odpovězeno ve většině případů do 12 hodin.

2.7 Veřejné klíče a informace o šifrování

CSIRT SZ podepisuje odchozí elektronické zprávy. Kromě toho CSIRT SZ dešifruje obdržené e-mailové zprávy a ověřuje, zda je digitální podpis zprávy validní.

Pro oznámení (hlášení) incidentu a související komunikaci prosím využijte níže uvedený klíč. Komunikační klíč (použijte pro ověření a šifrování):

- **User ID:** SŽ SOC <**soc@spravazeleznic.cz**>
- **Key ID:** D7DD CFAA 3C5D 46E1
- **Fingerprint:** E1A5 18B9 95FB 2E00 2727 9566 D7DD CFAA 3C5D 46E1

2.8 **Členové týmu**
Vedoucím týmu CSIRT SZ je Roman Kulich (Vedoucí odboru řízení událostí a incidentů). Kompletní přehled členů týmu není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují, a to druhé komunikující straně plným jménem.

Řízení a dohled CSIRT SZ je pověřen Ing. Lubošem Řádkem, MBA (Náměstek ředitele OJ pro kybernetickou bezpečnost, Manažer kybernetické bezpečnosti), Správy železniční telematiky.

2.9 **Další informace**
Obecné informace o CSIRT SZ lze nalézt na webových stránkách sdružení Trusted Introducer (dále jen „**TI**").[1]

2.10 **Kontakt s veřejností**
Preferovaný způsob kontaktování CSIRT SZ je prostřednictvím e-mailu. Oznámení (hlášení) incidentů a související otázky by měly být zaslány na e-mailovou adresu **soc@spravazeleznic.cz**. Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, obracejte se na CSIRT SZ telefonicky.

3 STANOVY

3.1 **Poslání**
CSIRT SZ hraje klíčovou roli při ochraně kritické infrastruktury Správy železnic, s.o. (dále jen „**SŽ**"). Naším cílem je účinně a efektivně čelit bezpečnostním hrozbám, reagovat na incidenty a koordinovat kroky k jejich úspěšnému vyřešení. Nedílnou součástí našeho poslání je účinné předcházení vzniku kybernetických bezpečnostních incidentů.

3.2 **Cílová skupina**
Naší cílovou skupinou jsou uživatelé, kteří využívají služeb Informačního systému Správy železnic, s.o.

3.3 **Zařazení**
CSIRT SZ slouží k ochraně informačního systému SŽ, kde vybrané subsystémy jsou součástí kritické informační infrastruktury Správy železnic, s.o., a to v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

3.4 **Oprávnění**
Vedení Správy železnic, s.o. plně podporuje činnost CSIRT SZ a je si vědomo důležitosti klíčových procesů a poskytovaných služeb Správy železnic, s.o. a nutností jejich ochrany proti kybernetickým hrozbám.

4 ZÁSADY

4.1 **Vnitřní předpisy**
CSIRT SZ jako součást Správy železnic, s.o. musí splňovat a dodržovat vnitřní předpisy a normy Správy železnic, s.o.

4.2 **Typy incidentů a úroveň podpory**
CSIRT SZ je oprávněn řešit veškeré typy incidentů tedy kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty, které vznikly nebo mohou potencionálně vzniknout v rámci kybernetického prostoru Správy železnic, s.o.

Úroveň podpory poskytované CSIRT SZ se liší v závislosti na typu a závažnosti incidentu či řešeného problému, typu původce, velikosti dotčené cílové uživatelské skupiny a zdrojích CSIRT SZ v daném okamžiku. Zvláštní pozornost je vždy věnována incidentům negativně ovlivňujícím kritickou informační infrastrukturu.

[1] Dostupné z https://www.trusted-introducer.org/

Podpora při řešení incidentů je poskytována primárně správcům (administrátorům) systémů a infrastruktury spadající do Správy železnic, s.o. Od koncových uživatelů se očekává aktivní spolupráce při řešení incidentů.

CSIRT SZ se zavazuje informovat o potenciálních zranitelnostech, a to v případech kdy je to možné, cílovou skupinu co nejrychleji, s cílem předejít možnému zneužití potenciální zranitelnosti.

4.3 **Spolupráce, interakce a zpřístupňování informací**
CSIRT SZ spolupracuje s dalšími organizacemi v oblasti počítačové bezpečnosti. Tato spolupráce zahrnuje a často vyžaduje výměnu důležitých informací týkajících se bezpečnostních incidentů a zranitelností.

S veškerými informacemi týkajících se kybernetických bezpečnostních incidentů a zranitelností nebo soukromí uživatelů atp. je zacházeno bezpečně a v souladu s právním řádem České republiky.

4.4 **Komunikace a autentizace**
Pro běžnou komunikaci neobsahující citlivé informace používá CSIRT SZ konvenční metody, jako je nešifrovaný e-mail.

Je-li nutné zaslat citlivé informace prostřednictvím e-mailu, bude ze strany CSIRT SZ používáno a vyžadováno šifrování za pomoci PGP.

Je-li nutné prověřit (autentizovat) osobu před zahájením komunikací, může tak být provedeno buď prostřednictvím existující sítě důvěry (např. TI nebo FIRST[2]), případně lze využít jiné metody jako je např. zpětné volání či zpětný e-mail nebo osobní setkání.

5 SLUŽBY

5.1 **Reakce na incidenty**
CSIRT SZ si klade za cíl aktivně pomáhat při řešení technických a organizačních aspektů kybernetických bezpečnostních incidentů. Zejména poskytuje odbornou podporu, nebo rady v případě krizového řízení.

5.2 **Třídění incidentů**
CSIRT SZ posuzuje závažnost jednotlivých incidentů pomocí taxonomie dle typu hrozby a rozsahu jeho dopadu.

5.3 **Koordinace při řešení incidentu**
CSIRT SZ kontaktuje zúčastněné strany (např. národní a zahraniční CERT a CSIRT týmy) v případě nutnosti, při řešení a prošetřování incidentu a následné možnosti přijetí příslušných nápravných opatření.

5.4 **Řešení incidentů**
CSIRT SZ při řešení incidentů poskytuje poradenství a navrhuje vhodný postup řešení vedoucích k eliminaci incidentu. Zejména poskytuje pomoc při shromažďování důkazů a při interpretaci dat, dále shromažďuje statistické údaje o událostech, které se dějí v rámci jeho pole působnosti, tedy kyberprostoru Správy železnic, s.o. Provádí informování o možných útocích a napomáhá při ochraně proti známým typům kybernetických útoků.

5.5 **Proaktivní přístup**
CSIRT SZ v rámci vzdělávání a zvyšování povědomí o informační a kybernetické bezpečnosti pravidelně školí svou cílovou skupinu a pravidelně publikuje oznámení o závažných bezpečnostních hrozbách s cílem zabránit možnému vzniku incidentu a snížit možný dopad.

Oznámení jsou publikována na intranetových a případně internetových stránkách Správy železnic, s.o.

[2] Dostupné z https://www.first.org/about/

6 ZPROŠTĚNÍ ODPOVĚDNOSTI

Navzdory všem opatřením, která jsou přijímána při přípravě vydávání oznámení, upozornění a varování, nepřebírá CSIRT SZ žádnou odpovědnost za chyby, opomenutí či škody vyplývající z využití informací, která tato oznámení, upozornění a varování obsahují.

Ing. Luboš Řádek MBA

Digitálně podepsal Ing. Luboš Řádek MBA
Datum: 2023.09.01 14:16:37 +02'00'

Ing. Luboš Řádek, MBA
náměstek Úseku kybernetické bezpečnosti
Správa železnic, státní organizace