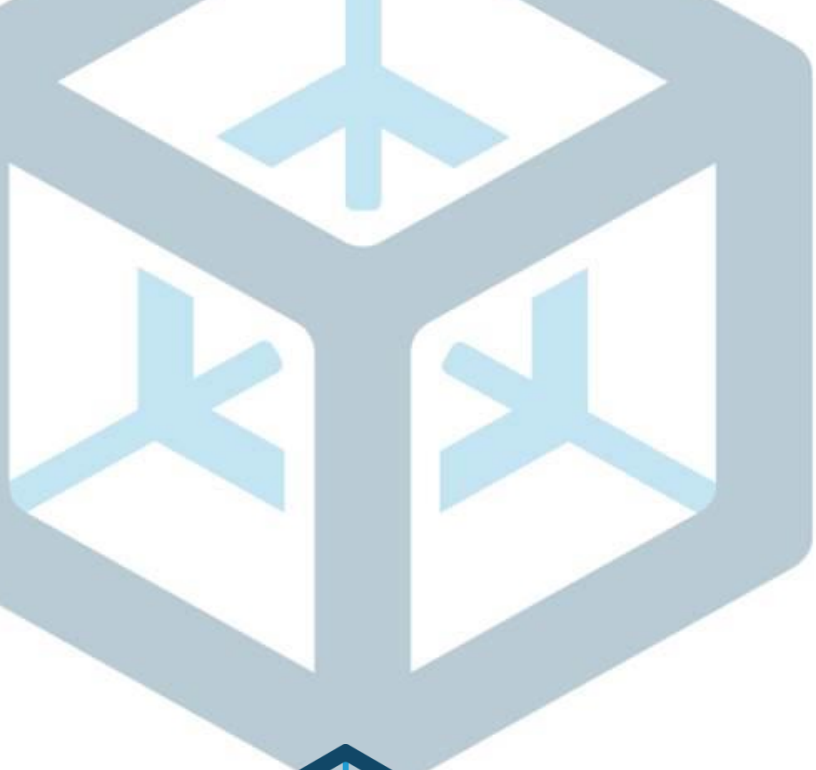

SPCSS

Státní pokladna
Centrum sdílených služeb

CENTRUM
KYBERNETICKÉ BEZPEČNOSTI

RFC 2350

CSIRT-SPCSS

TLP:CLEAR

1. O TOMTO DOKUMENTU

Tento dokument obsahuje popis CSIRT–SPCSS podle standardu RFC 2350. Poskytuje základní informace o CSIRT–SPCSS možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1. DATUM POSLEDNÍ AKTUALIZACE

Toto je verze číslo 3 ze dne 8.7.2022

1.2. DISTRIBUČNÍ SEZNAM PRO OZNÁMENÍ

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu CSIRT SPCSS s. p.

1.3 MÍSTA, KDE MŮŽE BÝT TENTO DOKUMENT NALEZEN

Aktuální verze tohoto popisného dokumentu CSIRT je dostupná na internetových stránkách Státní pokladny Centra sdílených služeb s. p.

2. KONTAKTNÍ INFORMACE

2.1 NÁZEV TÝMU

CSIRT–SPCSS

2.2 ADRESA

CSIRT–SPCSS

Na Vápence 14

138 00, Praha 3

Česká republika

2.3 ČASOVÉ PÁSMO

SEČ, 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

+420 225 515 990

2.5 OSTATNÍ TELEKOMUNIKACE

Není k dispozici

2.6 ELEKTRONICKÁ ADRESA

Pro hlášení incidentů prosím použijte adresu csirt@spcss.cz

Pro ostatní komunikaci prosím použijte adresu csirt@spcss.cz

2.7 VEŘEJNÉ KLÍČE A ŠIFROVACÍ INFORMACE

Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:

Pub:2048R/3AE09DD9

Fingerprint: 5229 049A 1853 B404 5CDE 1397 D071 F0B7 3AE0 9DD9

2.8 ČLENOVÉ TÝMU

Vedoucím týmu CSIRT–SPCSS s. p. je Mgr. Ondřej Nekovář. Kompletní přehled členů CSIRT není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

2.9 DALŠÍ INFORMACE

Obecné informace o CSIRT–SPCSS lze nalézt na stránce:
https://www.spcss.cz/csirt/

2.10 KONTAKT S VEŘEJNOSTÍ

Preferovaný způsob kontaktování CSIRT–SPCSS je prostřednictvím e-mailu.

Hlášení incidentů a související otázky by měly být zaslány na adresu csirt@spcss.cz. Tím se vytvoří hlášení v našem systému.

V případě ostatních dotazů prosím zašlete e-mail na csirt@spcss.cz

Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, můžete CSIRT–SPCSS kontaktovat telefonicky.

Pracovní doba CSIRT–SPCSS je v režimu 24/7/365

3. STANOVY

3.1 POSLÁNÍ

CSIRT–SPCSS hraje klíčovou roli při ochraně kritické informační infrastruktury Státní pokladny centra sdílených služeb a jejich zákazníků. Naším cílem je zlepšovat bezpečnost, obranu a ochranu infrastruktury a dat společnosti a minimalizovat dopad, který mohou způsobit průniky nebo kompromitace.

3.2 CÍLOVÁ SKUPINA

Naší cílovou skupinou je KII SPCSS 01 Bezpečné datové centrum SPCSS a Informační sys-témy vedené pod ASN AS203165.

3.3 ZAŘAZENÍ

CSIRT–SPCSS je součástí státního podniku Státní pokladna Centrum sdílených služeb s. p.

3.4 OPRÁVNĚNÍ

CSIRT–SPCSS pracuje pod záštitou a s pověřením Státní pokladny
Centra sdílených služeb s. p. SPCSS s. p. operuje v mezích české legislativy.

CSIRT–SPCSS plánuje spolupráci se správci systémů a uživateli v rámci institucí veřejného sektoru a kritické informační infrastruktury, jakož i s jinými subjekty s globálním dopadem.

4. ZÁSADY

4.1 TYPY INCIDENTŮ A ÚROVEŇ PODPORY

CSIRT–SPCSS je oprávněn řešit všechny typy počítačových bezpečnostních incidentů, které vznikly nebo mohou potenciálně vzniknout, v rámci jeho působnosti.

Úroveň podpory poskytnuté CSIRT–SPCSS se liší v závislosti na typu a závažnosti incidentu nebo problému, typ původce, velikosti uživatelské komunity a zdrojů CSIRT–SPCSS v okamžiku incidentu, ale v každém případě bude poskytnut nějaký typ reakce během jednoho pracovního dne. Zvláštní pozornost bude věnována incidentům, týkajícím se kritické informační infrastruktury.

Koncovým uživatelům může být poskytnuta přímá podpora.

CSIRT–SPCSS se zavazuje informovat o potenciálních zranitelnostech, a tam, kde je to možné, informovat výše zmíněnou cílovou skupinu o takových zranitelnostech ještě před jejich zneužitím.

4.2 SPOLUPRÁCE, INTERAKCE A ZPŘÍSTUPŇOVÁNÍ INFORMACÍ

S veškerými příchozími informacemi je nakládáno bezpečně, bez ohledu na jejich závažnost.

Informace, které jsou viditelně velmi citlivé povahy, budou zpracovávány a ukládány bezpečně, v případě nutnosti jsou využívány šifrovací technologie.

CSIRT–SPCSS bude využívat informace, které mu budou poskytnuty k řešení bezpečnostních incidentů.

Informace budou dále distribuovány ostatním týmům a členům pouze na základě principu need-to-know, a když to bude možné vždy anonymně.

4.3 KOMUNIKACE A AUTENTIZACE

E-maily a telefony jsou považovány za dostatečně bezpečný způsob, použitelný nešifrovaně, při přenosu málo citlivých dat. Je-li nutné zaslat vysoce citlivé údaje prostřednictvím e-mailu, bude využito šifrování PGP.

Je-li nutné prověřit osobu před zahájením komunikace, může tak být provedeno buď prostřednictvím existující sítě důvěry (např. TI, FIRST) nebo jinými metodami, jako je například zpětné volání, zpětný mail nebo, v případě potřeby, osobní setkání.

5. SLUŽBY

5.1 REAKCE NA INCIDENTY

CSIRT–SPCSS si klade za cíl pomáhat místním správcům při řešení technických a organizačních aspektů incidentů. Zejména plánuje poskytovat pomoc nebo rady s ohledem na následující aspekty krizového řízení:

5.1.1. TŘÍDĚNÍ INCIDENTŮ

- Posouzení, zda je incident věrohodný
- Určení rozsahu incidentu a jeho priority

5.1.2. KOORDINACE PŘI ŘEŠENÍ INCIDENTU

- Kontaktování zúčastněných stran incidentu k prošetření incidentu a následné přijetí příslušných opatření
- Usnadnění kontaktu s dalšími subjekty, které mohou pomoci s řešením incidentu
- Informování ostatních CERT® a CSIRT týmů v případě potřeby
- Komunikace se zúčastněnými stranami a médii

5.1.3. ŘEŠENÍ INCIDENTU

- Poskytování poradenství o vhodných postupech lokálním bezpečnostním týmům
- Sledování pokroku lokálních bezpečnostních týmů
- Poskytování pomoci při shromažďování důkazů a interpretaci dat

Kromě toho si klade CSIRT–SPCSS za cíl shromažďování statistických údajů o událostech, které se dějí v rámci jeho pole působnosti, včasné informování o možných útocích a napomáhání při ochraně proti známým útokům.

5.2 PROAKTIVNÍ PŘÍSTUP

CSIRT–SPCSS shromažďuje seznamy bezpečnostních kontaktů pro každou entitu v rámci svého pole působnosti. Tyto seznamy jsou k dispozici v případě potřeby při řešení bezpečnostních incidentů nebo útoků.

CSIRT–SPCSS publikuje oznámení o závažných bezpečnostních hrozbách, aby se v nejvyšší možné míře zabraňovalo incidentům v oblasti informačních a komunikačních technologií a snížil se tak co nejvíce jejich dopad.

CSIRT–SPCSS zpracovává IoC z dostupných zdrojů a v případě pozitivního nálezu zajišťuje předání relevantní informace kontaktu zodpovědnému za postižený systém.

CSIRT–SPCSS se také snaží zvyšovat povědomí o bezpečnosti v rámci svého pole působnosti.

6. FORMULÁŘE PRO HLÁŠENÍ INCIDENTŮ

Formulář pro nahlášení incidentu:

https://www.spcss.cz/csirt/

Pro alternativní formu hlášení (mailem na csirt@spcss.cz, telefonem na +420 225 515 990) uveďte následující skutečnosti:

- datum, čas a místo zjištění

- jméno a kontaktní informace zadavatele
- co nejpřesnější popis hlášené události (jak byla detekována / rozpoznána, možné příčiny, existující a odhadované dopady / škody)

7. ZPROŠTĚNÍ ODPOVĚDNOSTI

Navzdory všem opatřením, která budou přijata v přípravě oznámení informací, upozornění a varování, nepřebírá CSIRT–SPCSS žádnou odpovědnost za chyby, opomenutí, či škody, vyplývající z využití v nich obsažených informací.