TOTALSERVICE

Vaše ICT bez starostí

Popis

TS CSIRT

(TOTAL SERVICE CSIRT)

dle RFC 2350 standardu

TOTALSERVICE
Vaše ICT bez starostí

1. Obsah

2. O tomto dokumentu

Tento dokument obsahuje popis TOTAL SERVICE CSIRT (TS CSIRT) podle standardu RFC 2350. Poskytuje základní informace o TS CSIRT, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

2.1. Datum poslední aktualizace

Toto je verze číslo 3 ze dne 23. 02. 2020.

2.2. Distribuční seznam pro oznámení

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

2.3. Místa, kde může být tento dokument nalezen

Aktuální verze tohoto popisného dokumentu TS CSIRT je dostupná na internetových stránkách TOTAL SERVICE a.s. zde.

3. Kontaktní informace

3.1. Název týmu

TOTAL SERVICE CSIRT (zkráceně TS CSIRT)

3.2. Adresa

TOTAL SERVICE a.s. - CSIRT

Metropolitan Building

U Uranie 954/18

170 00 Praha 7

Česká republika

3.3. 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)

3.4. Telefonní číslo

+420 270 002 800

3.5. Faxové číslo

Není k dispozici

3.6. Ostatní komunikace

Není k dispozici

3.7. Elektronická adresa

Pro hlášení incidentů prosím použijte adresu csirt@totalservice.cz

Pro ostatní komunikaci prosím použijte adresu csirt@totalservice.cz

3.8. Veřejné klíče a šifrovací informace

Pro hlášení incidentu i ostatní komunikaci prosím použijte tento klíč:

User ID: Total Service CSIRT <csirt@totalservice.cz>

Fingerprint: D010 BA0C F8D5 EB99 E83B DA9F 9A33 FCE1 ED27 BEEA

Key type: RSA/4096

Expires: 2023-02-20

3.9. Členové týmu

Vedoucím týmu TS CSIRT je Radim Navrátil. Kompletní přehled členů týmu TS CSIRT není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

Řízení a dohled jsou zajišťovány vedoucím týmu.

3.10. Další informace

Obecné informace o TS CSIRT lze nalézt na stránce www.totalservice.cz

3.11. Kontakt s veřejností

Preferovaný způsob kontaktování TS-SCIRT je prostřednictvím e-mailu.

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

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

Pracovní doba TS CSIRT je obecně omezena na běžnou pracovní dobu (08:30-17:00 od pondělí do pátku, s výjimkou svátků).

4. Stanovy

4.1. Poslání

TS CSIRT tým si klade za cíl pomáhat při ochraně informační infrastruktury svých klientů a partnerů. Naším cílem je pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

4.2. Cílová skupina

Naší cílovou skupinou jsou především klienti společnosti TOTAL SERVICE a.s.

Zaměřujeme se na komerční, příspěvkové a neziskové společnosti a státní instituce.

4.3. Zařazení

TS CSIRT je součástí společnosti TOTAL SERVICE a.s., která je jeho provozovatelem.

4.4. Oprávnění

TS CSIRT pracuje v soukromém sektoru v mezích české a evropské legislativy.

TS CSIRT plánuje spolupráci se správci systémů a uživateli v rámci institucí soukromého i veřejného sektoru.

5. Zásady

5.1. Typy incidentů a úroveň podpory

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

Úroveň podpory poskytnuté TS CSIRT se liší v závislosti na typu a závažnosti incidentu nebo problému, velikosti uživatelské komunity a zdrojů TS CSIRT 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.

Žádná přímá podpora nebude poskytována koncovým uživatelům. Od nich se očekává spolupráce s jejich správcem systému, správcem sítě nebo provozovatelem internetových služeb. Právě těm poskytne TS CSIRT potřebnou podporu.

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

5.2. 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.

TS CSIRT 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.

TS CSIRT operuje v mezích české legislativy.

5.3. Komunikace a autentizace

Nešifrované e-maily a telefony jsou považovány za dostatečně bezpečný způsob komunikace 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.

6. Služby

6.1. Reakce na incidenty

TS CSIRT 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:

6.1.1. Třídění incidentů

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

6.1.2. 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.

6.1.3. 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 TS CSIRT 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.

6.2. Proaktivní přístup

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

TS CSIRT 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.

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

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

7. Formuláře pro hlášení incidentů

Nejsou k dispozici

8. Zproštění odpovědnosti

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