RFC 2350 STANDARD

POPIS TÝMU CSOC LKPR

1. TOMTO DOKUMENTU

Tento dokument obsahuje popis TÝMU CSOC LKPR podle standardu RFC 2350. Poskytuje základní informace o TÝMU CSOC LKPR, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1. DATUM POSLEDNÍ AKTUALIZACE

Toto je verze číslo 4 ze dne 01. 05. 2023.

1.2. DISTRIBUČNÍ SEZNAM PRO OZNÁMENÍ

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu tymu CSOC LKPR.

1.3. MÍSTA, KDE MŮŽE BÝT TENTO DOKUMENT NALEZEN

Aktuální verze tohoto popisného dokumentu CERT je dostupná na internetových stránkách týmu CSOC LKPR.

2. KONTAKTNÍ INFORMACE

2.1. NÁZEV TÝMU

CSOC LKPR: CSOC tým Letiště Praha

2.2. ADRESA

CSOC LKPR
Jana Kašpara 1069/1
161 00 Praha 6-Ruzyně
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

+420 220 111 155
Linka je dostupná v režimu 24 / 7 / 365

2.5. OSTATNÍ TELEKOMUNIKACE

Není k dispozici

2.6. ELEKTRONICKÁ ADRESA

Pro hlášení incidentů i běžnou komunikaci prosím použijte adresu csoc@prg.aero Na email je odpovídáno ve většině případů do 12 hodin.

2.7. VEŘEJNÉ KLÍČE A ŠIFROVACÍ INFORMACE

Pro hlášení incidentu a související komunikaci prosím použijte níže uvedený klíč.
Komunikační klíč (použijte pro ověřování a šifrování):
User ID: CSOC-LKPR <csoc@prg.aero>
Key ID: 0x74F4 C68E 0F93 F9D4
Fingerprint: 0x9706 43B8 B539 2DBF 3634 9F25 74F4 C68E 0F93 F9D4

2.8. ČLENOVÉ TÝMU

Vedoucím týmu Vládního CERT je Stanislav Petrák. Kompletní přehled členů týmu není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.
Řízení a dohled jsou poskytovány Romanem Palkovičem, ředitelem útvaru informační bezpečnosti Letiště Praha, a.s.

2.9. DALŠÍ INFORMACE

Obecné informace o CSOC LKPR lze nalézt na stránkách týmu.

2.10. KONTAKT S VEŘEJNOSTÍ

Preferovaný způsob kontaktování CSOC LKPR je prostřednictvím e-mailu.
Hlášení incidentů a související otázky by měly být zaslány na adresu csoc@prg.aero. Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, můžete CSOC LKPR kontaktovat telefonicky.
Pracovní doba CSOC LKPR je 24 / 7 / 365.

3. STANOVY

3.1. POSLÁNÍ

CSOC LKPR hraje klíčovou roli při ochraně kritické informační infrastruktury a systémů základní služby v rámci své konstituence. Naším cílem je účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

3.2. CÍLOVÁ SKUPINA

Naší cílovou skupinou jsou subjekty provozující služby na infrastruktuře spadající do naší konstituence.

3.3. ZAŘAZENÍ

CSOC LKPR je týmem spravujícím kritickou informační infrastrukturu a s ní související systémy základní služby dle zákona č. 181/2014 Sb.

3.4. OPRÁVNĚNÍ

CSOC LKPR pracuje pod záštitou vedení společnosti Letiště Praha, a.s. , které operuje v rámci platné legislativy ČR.
CSOC LKPR spolupracuje s Vládním CERTem a dalšími subjekty sdruženými v rámci bezpečnostní komunity.

4. ZÁSADY

4.1. TYPY INCIDENTŮ A ÚROVEŇ PODPORY

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

Úroveň podpory poskytnuté CSOCem LKPR se liší v závislosti na typu a závažnosti incidentu, nebo problému, typu původce, velikosti uživatelské komunity a zdrojů CSOCu 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.

Podpora je poskytována výhradně správcům systémů a infrastruktury. Od koncových uživatelů se očekává spolupráce s jejich správcem systému, správcem sítě, nebo provozovatelem internetových služeb.

CSOC LKPR 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.

CSOC LKPR 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.

CSOC LKPR operuje v mezích české legislativy, upřesněných interními předpisy.

4.3. KOMUNIKACE A AUTENTIZACE

Nešifrované E-maily a telefony jsou považovány za dostatečně bezpečný způsob komunikace pouze pro předávání méně 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

CSOC LKPR si klade za cíl pomáhat místním správcům při řešení technických a organizačních aspektů incidentů. Zejména poskytuje 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 CSOC týmů v případě potřeby. Komunikace se zúčastněnými stranami a médii.

5.1.3. ŘEŠENÍ INCIDENTU

Poskytování poradenství správcům o vhodných postupech.
Sledování pokroku řešení správců informačních technologií a infrastruktury.
Poskytování pomoci při shromažďování důkazů a interpretace dat. Kromě toho CSOC LKPR shromažďuje statistické údaje 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

CSOC LKPR 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.
CSOC LKPR 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. Oznámení jsou na intranetových stránkách konstituenta v sekci o útvaru IBE.
CSOC LKPR zpracovává IoC (Indicator of Compromise) z dostupných zdrojů a v případě pozitivního nálezu zajišťuje předání relevantní informace kontaktu zodpovědnému za postižený systém.
CSOC se také snaží zvyšovat povědomí o bezpečnosti v rámci svého pole působnosti.

6. ZPROŠTĚNÍ ODPOVĚDNOSTI

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