POPIS VLÁDNÍHO CERT ČESKÉ REPUBLIKY

1. O TOMTO DOKUMENTU

Tento dokument obsahuje popis Vládního CERT České republiky podle standardu RFC 2350. Poskytuje základní informace o Vládním CERT, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1 DATUM POSLEDNÍ AKTUALIZACE

Toto je verze číslo 12 ze dne 17. 8. 2020.

1.2 DISTRIBUČNÍ SEZNAM PRO OZNÁMENÍ

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

1.3 MÍSTA, KDE MŮŽE BÝT TENTO DOKUMENT NALEZEN

Aktuální verze tohoto popisného dokumentu CERT je dostupná na internetových stránkách Vládního CERT – ke stažení zde

2. KONTAKTNÍ INFORMACE

2.1 NÁZEV TÝMU

GovCERT.CZ: Vládní CERT České republiky

2.2 ADRESA

Národní centrum kybernetické bezpečnosti (Vládní CERT)
Mučednická 1125/31
616 00, Brno
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

+420 541 110 777

+420 725 502 878 (mimo pracovní dobu)

2.5 FAXOVÉ ČÍSLO

+420 257 283 580

2.6 OSTATNÍ TELEKOMUNIKACE

Není k dispozici

2.7 ELEKTRONICKÁ ADRESA

Pro hlášení incidentů prosím použijte adresu cert.incident@nukib.cz.

Pro ostatní komunikaci prosím použijte adresu cert@nukib.cz.

2.8 VEŘEJNÉ KLÍČE A ŠIFROVACÍ INFORMACE

Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:

```
pub  4096R/D2A1C881 2019-08-01
uid Government CERT Incident CZE (Reporting channel for NCSC CZE)
<cert.incident@nukib.cz>
Key fingerprint = 3F29 12FE 999B 93D9 AB58 DC5C 43A1 3897 D2A1 C881
```

Pro ostatní komunikaci prosím použijte tento klíč:

```
pub  4096R/A57337A6 2019-08-01
uid Government CERT CZE (Communication channel with NCSC CZE)
<cert@nukib.cz>
Key fingerprint = F60C 0622 EE75 52C9 7EE5 E9F8 4405 4AC1 A573 37A6
```

2.9 ČLENOVÉ TÝMU

Vedoucím týmu a zároveň ředitelem odboru Vládní CERT je Jakub Veselý. Kompletní přehled členů týmu Vládního CERT není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

Řízení a dohled provádí Lukáš Kintr, náměstek Národního centra kybernetické bezpečnosti Národního úřadu pro kybernetickou a informační bezpečnost.

2.10 DALŠÍ INFORMACE

Obecné informace o Vládním CERT lze nalézt na stránce www.nukib.cz.

2.11 KONTAKT S VEŘEJNOSTÍ

Preferovaný způsob kontaktování Vládního CERT je prostřednictvím e-mailu.

Hlášení incidentů a související otázky by měly být zaslány na adresu cert.incident@nukib.cz. Tím se vytvoří hlášení v našem systému. V případě hlášení incidentu mimo pracovní dobu navíc kontaktujte pracovníka vykonávajícího pohotovost na čísle +420 725 502 878.

V případě ostatních dotazů prosím zašlete e-mail na cert@nukib.cz.

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

Pracovní doba Vládního CERT je obecně omezena na běžnou pracovní dobu (07:45-16:30 od pondělí do pátku, s výjimkou svátků).

3. STANOVY

3.1 POSLÁNÍ

Vládní CERT hraje klíčovou roli při ochraně kritické informační infrastruktury a státních orgánů. Naším cílem je pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

3.2 CÍLOVÁ SKUPINA

Naší cílovou skupinou jsou veřejné instituce a kritická informační infrastruktura v České republice.

3.3 ZAŘAZENÍ

Vládní CERT je součástí Národního centra kybernetické bezpečnosti Národního úřadu pro kybernetickou a informační bezpečnost České republiky.

3.4 OPRÁVNĚNÍ

Vládní CERT pracuje pod záštitou a s pověřením Národního centra kybernetické bezpečnosti. Národní centrum kybernetické bezpečnosti operuje v mezích české legislativy.

Vládní CERT plánuje spolupráci se správci systémů a uživateli v rámci institucí veřejného sektoru a kritické informační infrastruktury.

4. ZÁSADY

4.1 TYPY INCIDENTŮ A ÚROVEŇ PODPORY

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

Úroveň podpory poskytnuté Vládním CERT se liší v závislosti na typu a závažnosti incidentu nebo problému, typ původce, velikosti uživatelské komunity a zdrojů Vládního CERT 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 Vládní CERT potřebnou podporu.

Vládní CERT 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.

Vládní CERT 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.

Vládní CERT operuje v mezích české legislativy.

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

Vládní CERT 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 Vládní CERT 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

Vládní CERT 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.

Vládní CERT 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.

Vládní CERT zpracovává IoC[1] z dostupných zdrojů a v případě pozitivního nálezu zajišťuje předání relevantní informace kontaktu zodpovědnému za postižený systém.

Vládní CERT se také snaží zvyšovat povědomí o bezpečnosti v rámci svého pole působnosti.

6. FORMULÁŘE PRO HLÁŠENÍ INCIDENTŮ

Formulář je ke stažení zde

XML schéma je dostupné zde

7. ZPROŠTĚNÍ ODPOVĚDNOSTI

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

[1] Indicator of Compromise