RFC2350 - Popis CSIRT Skupiny ČEZ

1. O tomto dokumentu

Tento dokument obsahuje informace, týkající se řešení skupinově významných incidentů v oblasti kybernetické bezpečnosti ve Skupině ČEZ. Dokument je koncipován podle standardu RFC 2350 a poskytuje základní informace o CSIRT-CEZ, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1 Datum poslední aktualizace

Toto je verze číslo 1 ze dne 7.2.2023

1.2 Distribuční seznam pro oznámení

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

1.3 Možnost stáhnout tento dokument

Aktuální verze tohoto dokumentu je umístěna na internetových stránkách Skupiny ČEZ

2. Kontaktní informace

2.1 Název týmu

CSIRT-CEZ

2.2 Adresa

CSIRT-CEZ
Duhová 2/1444
Praha 4, 140 53
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

+420 211 042 699 (mimo standardní pracovní dobu je toto telefonní číslo přesměrováno na pohotovost)

2.5 Faxové číslo

Není k dispozici

2.6 Ostatní telekomunikace

Není k dispozici

2.7 Elektronická adresa

Pro veškerou komunikaci s CSIRT-CEZ včetně hlášení incidentů prosím použijte adresu csirt@cez.cz.

2.8 Veřejné klíče a šifrovací informace

Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:

Type: RSA/3072 Expires: 16.1.2028

Fpr: 12E8 74DE DBF3 4F1F 7EFE 92CB FF1A 27C4 F49B BA2B

UID: CSIRT-CEZ csirt@cez.cz.

2.9 Členové týmu

Vedoucím týmu CSIRT-CEZ je Tomáš Grznár (tomas.grznar@cez.cz). Kompletní přehled členů týmu CSIRT-CEZ není veřejně k dispozici.

Členové týmu se při oficiální komunikaci ohledně incidentu představí protistraně plným jménem.

2.10 DALŠÍ INFORMACE

Preferovaný způsob kontaktování CSIRT-CEZ je prostřednictvím e-mailu.

Není-li možné (nebo není-li to z bezpečnostního hlediska vhodné) použít e-mail, můžete CSIRT-CEZ kontaktovat telefonicky na výše uvedených číslech.

Pracovní doba CSIRT-CEZ je obecně omezena na běžnou pracovní dobu (08:00-16:00 od pondělí do pátku, s výjimkou svátků). Mimo pracovní dobu je zajištěna pohotovost.

3. Stanovy

3.1 Poslání

CSIRT-CEZ řeší skupinově významné incidenty z oblasti kybernetické bezpečnosti v rámci provozovaných sítí a systémů Skupiny ČEZ. 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 všechny společnosti Skupiny ČEZ, které přistupují do kybernetického prostoru Skupiny ČEZ nebo využívají její IT prostředky, a které nemají vlastní kapacity a prostředky pro zvládání významných incidentů z oblasti kybernetické bezpečnosti.

3.3 Zařazení

CSIRT-CEZ je součástí útvaru Ochrana Skupiny ČEZ ve společnosti ČEZ, a. s.

3.4 Oprávnění

CSIRT-CEZ má mandát od vedení společnosti řídit a podporovat zvládání skupinově významných incidentů z oblasti kybernetické bezpečnosti.

CSIRT-CEZ spolupracuje při řešení bezpečnostních incidentů primárně s Národním centrem kybernetické bezpečnosti (vládní CERT) nebo s dalšími CERT/CSIRT týmy v rámci Skupiny ČEZ.

4. Zásady

4.1 Typy incidentů a úroveň podpory

CSIRT-CEZ řeší incidenty, které vzniknou v kyberprostoru Skupiny ČEZ, a mají skupinově významný dopad. Za skupinově významné incidenty jsou považovány takové, které:

- mají významný dopad do fungování většího počtu společností Skupiny ČEZ a/nebo
- jsou výsledkem dlouhodobého koordinovaného útoku cíleného na Skupinu ČEZ a/nebo
- probíhají souběžně nebo jsou příčinou krize, kvůli které byl aktivován krizový štáb ČEZ a/nebo
- pro zmírnění jejich dopadů je nutné přijímat rozhodnutí, které mohou mít dopad do podnikatelských aktivit většího množství společností Skupiny ČEZ (např. omezení konektivity do internetu, omezení dostupnosti většího množství centrálních systémů) a to včetně tech, které nebyly přímými cíli kybernetického útoku.

Úroveň podpory poskytnuté CSIRT-CEZ se liší v závislosti na typu a závažnosti incidentu nebo problému, typ původce, velikosti uživatelské komunity a dostupnosti zdrojů CSIRT-CEZ v okamžiku incidentu. Zvláštní pozornost bude věnována incidentům, týkajícím se kritické informační infrastruktury.

Pro společnosti Skupiny ČEZ, které mají vybudovány vlastní kapacity pro zvládání incidentů z oblasti kybernetické bezpečnosti, nebo pro společnosti Skupiny ČEZ, které nepřistupují do kyberprostoru Skupiny ČEZ ani nevyužívají IT prostředky Skupiny ČEZ, bude CSIRT-CEZ poskytovat zejména konzultační a metodickou podporu.

CSIRT-CEZ 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

CSIRT-CEZ je připraven spolupracovat s ostatními důvěryhodnými bezpečnostními týmy v ČR i zahraničí.

S informacemi získanými v rámci činnosti CSIRT-CEZ nebo sdílenými v rámci komunity bezpečnostních týmu bude nakládáno v souladu s požadavky české legislativy.

4.3 Komunikace a autentizace

E-maily a telefony jsou považovány za dostatečně bezpečný způsob komunikace, použitelné 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-CEZ si klade za cíl poskytovat podporu místním správcům ve společnostech Skupiny ČEZ při řešení technických a organizačních aspektů incidentů v oblasti kybernetické bezpečnosti. Bude poskytovat odbornou pomoc a součinnost v rámci následujících typů činností:

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.

5.1.3. ŘEŠENÍ INCIDENTU

- Poskytování odborné pomoci a součinnosti o vhodných postupech zapojených bezpečnostním týmům jednotlivých společností Skupiny ČEZ
- Dohled nad postupem řešení incidentu zapojených bezpečnostních týmů jednotlivých společností Skupiny ČEZ
- Definice opatření/aktivit k ochraně systémů a dalších IT prostředků Skupiny ČEZ před dopadem incidentu
- Definice nápravných opatření k odstranění zjištěných zranitelností a dozorování realizace těchto opatření.

5.2 Proaktivní přístup

CSIRT-CEZ se podílí na řadě proaktivních činností vedoucích ke zvýšení bezpečnostního povědomí ve společnostech Skupiny ČEZ.

6. Zproštění odpovědnosti

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