1. O tomto dokumentu

Tento dokument obsahuje popis týmu O2 Czech Republic CERT podle standardu RFC 2350. Poskytuje základní informace o O2 Czech Republic CERT, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1 Datum poslední aktualizace

Toto je verze číslo 2 ze dne 23. 8. 2023.

1.2 Distribuční seznam pro oznámení

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na emailovou adresu týmu O2 Czech Republic CERT cert@o2.cz.

1.3 Místa, kde může být tento dokument nalezen

Aktuální verze tohoto popisného dokumentu CERT je dostupná ke stažení na https://www.o2.cz/soukromi/cert.

2. Kontaktní informace

2.1 Název týmu

O2 Czech Republic CERT (O2.cz CERT)

2.2 Adresa

(O2.cz CERT)
O2 Czech Republic a.s.
Za Brumlovkou 266/2
Praha 4 – Michle
140 22
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

+420 602 341 564

2.5 Faxové číslo

Není k dispozici

2.6 Ostatní telekomunikace

Není k dispozici

2.7 Elektronická adresa

Pro hlášení incidentů prosím použijte adresu abuse@o2.cz.
Pro ostatní komunikaci prosím použijte adresu cert@o2.cz.

2.8 Veřejné klíče a šifrovací informace

Pro šifrovanou komunikaci s O2.cz CERT prosím použijte tento klíč:
uid: O2.cz CERT (O2.cz CERT) cert@o2.cz
Key fingerprint: 98CC E6AF CCF7 D513 CEA5 1926 615B A4B5 CFEA CC7C
Veřejný klíč je stáhnutelný z https://www.o2.cz/soukromi/cert

2.9 Členové týmu

Vedoucím týmu O2.cz CERT a zároveň bezpečnostní ředitelem je Radek Šichtanc. Kompletní přehled členů týmu O2.cz CERT není veřejně k dispozici.

2.10 Další informace
Obecné informace o týmu O2.cz CERT lze nalézt na stránce https://www.o2.cz/soukromi/cert

2.11 Kontakt s veřejností
Preferovaný způsob kontaktování týmu O2.cz CERT je prostřednictvím e-mailu. Pro hlášení incident typu použijte adresu abuse@o2.cz. V případě ostatních dotazů zašlete e-mail na cert@o2.cz.
Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, můžete O2.cz CERT kontaktovat telefonicky na čísle +420 602 341 564
Pracovní doba O2.cz CERT je obecně omezena na běžnou pracovní dobu (09:00-17:00 od pondělí do pátku, s výjimkou svátků).

3. Stanovy
3.1 Poslání
Účelem O2.cz CERT je přispívat k bezpečnosti ICT infrastruktury společnosti prostřednictvím budování a udržování kapacit pro identifikaci, reakci a řešení problémů v oblasti počítačové a informační bezpečnosti. Naším cílem je pomáhat uživatelům sítě O2 Czech Republic při zavádění proaktivních opatření ke snížení rizik počítačových bezpečnostních incidentů a pomáhat jim při reakci na tyto incidenty, pokud k nim dojde.

3.2 Cílová skupina
Cílovou skupinou O2.cz CERT jsou všechny společnosti a uživatelé O2 Czech Republic (obsahuje všechny systémy připojené k síti O2 Czech Republic: AS5610, AS20884). Upozorňujeme však, že vzhledem k charakteru poskytovaných služeb uživatelům sítě O2 Czech Republic, různým typům cílových skupin je poskytována různá úroveň podpory (podrobnosti najdete v kapitolech 4.1 a 5.1)

3.3 Zařazení
O2.cz CERT je součástí společnosti O2 Czech Republic a.s.

3.4 Oprávnění
O2.cz CERT pracuje pod záštitou a s pověřením společnosti O2 Czech Republic a.s. O2.cz CERT je pověřen řízením a podporou řešení kybernetických bezpečnostních incidentů.

4. Zásady
4.1 Typy incidentů a úroveň podpory
O2.cz CERT je oprávněn řešit všechny typy kybernetických bezpečnostních incidentů, které se vyskytnou nebo hrozí v rámci cílové skupiny.

Úroveň podpory poskytnuté O2.cz CERT se liší v závislosti na typu a závažnosti incidentu nebo problému, typu původce, velikosti uživatelské komunity a dostupnosti zdrojů O2.cz CERT v okamžiku incidentu. O2.cz CERT přijme jakoukoli zprávu o incidentu, která zahrnuje incident související s některou z cílových skupin, zvláštní pozornost bude věnována incidentům, týkajícím se kritické informační infrastruktury. Pouze v případech, kdy se hlášení týká interní infrastruktury O2 Czech Republic, je však O2.cz CERT schopen se incidenty zabývat. V případě individuálních a B2B zákazníků je reakce na incidenty omezena pouze na kritické situace. Upozorňujeme, že koncovým uživatelům nebude poskytována přímá podpora; očekává se, že se obrátí na své správce systému, správce sítě nebo bezpečnostní manažery. O2.cz CERT bude poskytovat podporu těmto osobám.

O2.cz 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 sdělování informací
O2.cz CERT se řídí interními zásadami pro nakládání s daty, zásadami pro ochrany osobních údajů a deklaruje plnou podporu protokolu Information Sharing Traffic Light Protocol. O2.cz CERT může sdílet informace zaslané na základě potřeby vědět s důvěryhodnými stranami (jiné týmy CERT/CSIRT, jiní poskytovatelé internetových služeb) výhradně za účelem řešení incidentů.

S informacemi získanými v rámci činnosti O2.cz CERT nebo sdílenými v rámci komunity bezpečnostních týmu bude nakládáno v souladu výše uvedenými zásadami a v souladu s požadavky české legislativy.

4.3 Komunikace a autentizace
Pro běžnou komunikaci, která neobsahuje citlivé informace, lze použít e-mail. Pro zabezpečenou komunikaci se používá šifrovaný e-mail s využitím PGP.

5. Služby

5.1 Reakce na incidenty
O2.cz CERT zajišťuje veškeré technické a organizační aspekty reakce na incidenty. Poskytuje zejména následující služby:

5.1.1. Třídění incidentů
Hlavní cíle třídění incidentů jsou:
- šetření, zda skutečně došlo k bezpečnostnímu incidentu,
- určení rozsahu a závažnosti incidentu (včetně možného dopadu na cílové skupiny)

5.1.2. Koordinace při řešení incidentu
Cílem je poskytnout komplexní koordinaci incidentu mezi všemi zúčastněnými stranami.
Následujícím cílem je zajistit komplexní koordinaci mezi různými zúčastněnými stranami. To zahrnuje mimo jiné
- určení počáteční příčiny incidentu (využitá zranitelnost),
- kontaktování zúčastněných stran za účelem prošetření incidentu a přijetí příslušných opatření,
- zprostředkování kontaktu s dalšími stranami, které mohou pomoci incident vyřešit,
- podávání zpráv jiným skupinám CERT nebo CSIRT, je-li to nutné, a
- komunikace se zúčastněnými stranami a médii.

Vzhledem k omezeným zdrojům je tato služba primárně určena pro interní infrastrukturu O2 Czech Republic a B2B zákazníky. Ve velmi ojedinělých kritických situacích je koordinace incidentů poskytována jednotlivým zákazníkům.

5.1.3. Řešení incidentu
Řešení incidentů se provádí pouze v omezeném rozsahu, a to pro interní infrastrukturu O2 Czech Republic. Jedná se mimo jiné o:
- odstranění zranitelnosti,
- zabezpečení systému před následky incidentu,
- shromažďování důkazů a interpretaci dat,
- atp.

5.2 Proaktivní přístup
O2.cz CERT se podílí na aktivitách zaměřených na
- zvyšování bezpečnostního povědomí,
- veřejná oznámení týkající se závažných bezpečnostních hrozeb,
- sledování aktuálních trendů v oblasti technologií a bezpečnosti a
- šíření relevantních znalostí v rámci svého pole působnosti.

6. Formuláře pro hlášení incidentů
Pro účely hlášení incidentů nejsou k dispozici žádné specifické formuláře. Při hlášení incidentů pomocí e-mailu se řiďte následujícími základními pravidly:
- Hlášení musí obsahovat vaše kontaktní údaje a údaje o organizaci – jméno a příjmení oznamovatele, název organizace (pokud je relevantní), e-mail a telefonní číslo.
- Hlášení musí obsahovat IP adresu, typ incidentu, přibližný čas, kdy incident začal, kdy byl incident zjištěn, a logy relevantní pro daný problém (pokud jsou k dispozici).

- Hlášení o spamu (nebo škodlivé příloze e-mailu) musí obsahovat kopii úplné hlavičky e-mailu, který je považován za spam (nebo který obsahuje danou přílohu).
- Hlášení o phishingu nebo pharmingu musí obsahovat adresu URL a IP adresu webové stránky spolu s jejím zdrojovým kódem, je-li to možné.

7. Zproštění odpovědnosti

Navzdory všem opatřením, která budou přijata v přípravě oznámení informací, upozornění a varování, nepřebírá O2.cz CERT žádnou odpovědnost za chyby, opomenutí, či škody, vyplývající z využití v nich obsažených informací.