SOC365 CSIRT

1. O tomto dokumentu

Tento dokument obsahuje popis Security Operation Center 365 CSIRT podle RFC 2350. Poskytuje základní informace o týmu SOC365 CSIRT, způsobech, jakými jej lze kontaktovat, a popisuje nabízené služby.

1.1 Datum poslední aktualizace

Toto je verze číslo 2 ze dne 27. 05. 2024.

1.2. Distribuční seznam pro oznámení

Není k dispozici.

1.3 Místa, kde může být tento dokument nalezen

Aktuální verze tohoto popisného dokumentu je dostupná na internetových stránkách na odkaze: https://www.soc365.cz/wp-content/uploads/2024/05/RFC2350_SOC365_CSIRT_CZ.pdf

2. Kontaktní informace

2.1 Název týmu

Security Operation Center 365 CSIRT.

2.2 Adresa

Řípska 11c
627 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

+420 515 919 570.

2.5 Faxové číslo

+420 543 211 754.

2.6 Ostatní telekomunikace

Není k dispozici.

2.7 Elektronická adresa

Pro komunikaci prosím použijte csirt@soc365.cz

2.8 Veřejné klíče a šifrovací informace

Pro šifrovanou komunikaci prosím použijte csirt@soc365.cz

PGP key:
Type: RSA/4096 Expires: 2028-02-28
Fpr: 461A 982F 168F 3BE0 01C2 4B0C CDD1 D13F EAE2 DCE1
UID: CSIRT SOC365 <csirt@soc365.cz>

2.9 Členové týmu

Přehled členů týmu Vládního CERT není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

2.10 Další informace

Obecné informace naleznete na www.soc365.cz.

2.11 Kontakt s veřejností

Preferovaný způsob kontaktování Vládního CERT je prostřednictvím e-mailu.

Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, kontaktujte nás telefonicky.

3. Stanovy

3.1 Poslání

Naším cílem je proaktivně čelit kybernetickým bezpečnostním hrozbám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

3.2 Cílová skupina

Naší klientelou jsou instituce veřejného nebo soukromého sektoru a kritická informační infrastruktura České republiky a Slovenska.

4. Zásady

4.1 Typy incidentů a úroveň podpory

Přednastavená základní priorita pro všechny incidenty je normální priorita. Členové týmu CSIRT SOC365 provedou hlubší analýzu daného jevu, na jejímž základě provedou kategorizaci detekce a v případě potřeby aktivují proces reakce na incident podle stanovených parametrů.

4.2 Spolupráce, interakce a zpřístupnění informací

Veškeré příchozí informace jsou zpracovávány bezpečně bez ohledu na obsah nebo dopad. S citlivými informacemi se nakládá podle našeho klasifikačního schématu a v případě potřeby se používá kryptografie.

4.3 Komunikace a autentizace

PGP/GnuPG se používá pro veškerou citlivou komunikaci nebo přenos informací nebo jsou členové týmu instruováni, aby použili jakýkoli legální způsob autentizace (např. výzva třetímu subjektu k identifikaci).

5. Služby

5.1 Reakce na incidenty

Zpracování probíhá podle interní směrnice. Proces zahrnuje kategorizaci, ticketing a oznámení.

5.1.1. Třídění incidentů

- Posouzení důvěryhodnosti
- Klasifikace priority podle vyhlášky. 82/2018 Sb., vyhláška o kybernetické bezpečnosti.
- Přiřazení analytikovi nebo řešiteli

5.1.2. Koordinace při řešení incidentu

- Kontaktování zúčastněných stran incidentu k prošetření incidentu
- Přijetí příslušných opatření
- Pokud je to nezbytné, tak informovat ostatní členy týmu CSIRT

5.2 Proaktivní přístup

Pravidelně analyzujeme veřejné a poskytnuté informace o trendech a novinkách v oblasti kybernetické bezpečnosti. V případě zjištění relevantních informací je provedeno hlubší šetření a v případě potvrzení informací distribuujeme doporučení a varování.

6. Formulář pro hlášení incidentů

Formulář ke stažení zde.

7. Zproštění odpovědnosti

Žádné.