Dokument RFC 2350

Informácie o dokumente

Dokument obsahuje popis GOV CERT SK na základe RFC 2350.

1.1 Dátum poslednej aktualizácie

Toto je verzia 3.2 zo dňa 16.10.2025.

1.2 Distribučný zoznam pre oznámenia

V súvislosti so zmenami RFC 2350 neexistuje distribučný zoznam oznámení poskytovaný GOV CERT SK.

1.3 Miesta, kde je možné tento dokument nájsť

Aktuálna verzia dokumentu je dostupná na webovej stránke - https://cert.gov.sk/rfc-2350

PDF verzia dokumentu je dostupná na - https://cert.gov.sk/files/rfc-2350_sk.pdf

1.4 Overenie dokumentu

Tento dokument bol digitálne podpísaný pomocou PGP kľúča GOV CERT SK.
Podpis je dostupný na: https://cert.gov.sk/files/rfc-2350_sk.sig

Kontaktné informácie

2.1 Názov tímu

GOV CERT SK – Government Network Cyber Emergency Response Team Slovenská republika

2.2 Adresa

Národná agentúra pre sieťové a elektronické služby

GOV CERT SK

Tower 115

Pribinova 25

811 09 Bratislava

2.3 Časové pásmo

- CET – Stredoeurópsky čas (UTC+1, od poslednej októbrovej nedele do poslednej marcovej soboty)
- CEST – Stredoeurópsky letný čas (UTC+2, od poslednej marcovej nedele do poslednej októbrovej soboty)

2.4 Telefónne číslo

+421 (0)917 691 326

2.5 Fax

Nedostupné

2.6 Iné telekomunikačné spojenie

Nedostupné

2.7 Emailové adresy

Pre hlásenie incidentov prosím použiť adresu incident@cert.gov.sk

Pre inú komunikáciu prosím použiť adresu info@cert.gov.sk

2.8 Verejné kľúče a šifrovacie informácie

Pre komunikáciu súvisiacu s incidentmi môžete použiť tento kľúč:

- Identifikátor: GOV CERT SK (NASES)
- PGP Key ID: 0xBF27B9743EF0A6D9
- PGP Key Fingerprint: 0211 4DC5 1D3C E359 DE0C 988B BF27 B974 3EF0 A6D9
- Kľúč je dostupný na stiahnutie vo formáte TXT - https://cert.gov.sk/files/GOV-CERT-SK.pub

Certifikačná autorita GOV CERT SK

Verejné PGP kľúče pre bezpečnú komunikáciu sú podpísané certifikačnou autoritou GOV CERT SK.

- Identifikátor: GOV CERT SK (CA)
- PGP Key ID: 0x6D4AC34E7F63D9C6
- PGP Key Fingerprint: 7B64 D925 C0DB AE35 53ED E197 6D4A C34E 7F63 D9C6
- Kľúč je dostupný na stiahnutie vo formáte TXT tu https://cert.gov.sk/files/GOV-CERT-SK_CA.pub

2.9 Členovia tímu

Informácie o členoch GOV CERT SK nie sú zverejňované.

Riadenie zabezpečuje vedúci tímu GOV CERT SK **Radoslav Zlacký** a kontrolu vykonáva riaditeľ Bezpečnostnej divízie Národnej agentúry pre sieťové a elektronické služby **Norbert Skákala**.

Neoddeliteľnou súčasťou nami poskytovaných služieb je tím **NASES SOC**. Hoci tím SOC nie je formálne definovaný v organizačnej štruktúre NASES ako súčasť GOV CERT, zostáva neoddeliteľnou súčasťou poskytovania služieb GOV CERT.

2.10 Ďalšie informácie

Viac verejných informácií: https://cert.gov.sk

2.11 Kontakt s verejnosťou

- Preferovaná forma kontaktu: e-mail.
- Všeobecné otázky: info@cert.gov.sk
- Hlásenie incidentov: incident@cert.gov.sk
- Ak nie je možné použiť e-mail (alebo z bezpečnostných dôvodov), môžete volať na číslo +421 (0)917 691 326 (24/7).

Stanovy

3.1 Poslanie

GOV CERT SK pôsobí pri ochrane základných a kritických služieb NASES, ako aj pri ochrane centrálnej informačnej a komunikačnej infraštruktúry verejnej správy Slovenskej republiky.

3.2 Pôsobnosť

- Služby pre GOVNET (vládna sieť SR), Ústredný portál verejnej správy, vybrané orgány verejnej správy a ďalšie projekty a IS spravované NASES.

- Služby monitorovania a detekcie incidentov v rámci Govnetu a pre vybrané OVM.
- Ochrana bezpečnosti ÚPVS je kľúčová aj pre bezpečnosť údajov NGO a občanov – koncových používateľov portálu.

3.3 Zriaďovateľ a/alebo príslušnosť

GOV CERT SK je súčasťou Národnej agentúry pre sieťové a elektronické služby.

3.4 Autorita

GOV CERT SK pôsobí v súlade so štatútom NASES a spolupracuje so správcami a prevádzkovateľmi IS verejného sektora.

Politiky

4.1 Typy incidentov a úroveň podpory

- GOV CERT SK rieši všetky typy bezpečnostných incidentov v rámci svojej pôsobnosti.
- Úroveň podpory sa odvíja od závažnosti, pôvodu, veľkosti postihnutej komunity a dostupných zdrojov.
- Pomoc je poskytovaná čo najrýchlejšie, ale priamo sa nepodporujú koncoví používatelia – len administrátori IS verejnej správy.
- GOV CERT SK upozorňuje na zraniteľnosti a ak je možné, informuje o nich vopred.

4.2 Spolupráca, interakcia a zverejňovanie informácií

- Všetky informácie sú spracúvané v súlade so zákonmi SR.

- Citlivé údaje sú spracované podľa klasifikácie.
- Informácie sa využívajú výlučne na riešenie incidentov a ďalej sa distribujú len na princípe „need-to-know“, ak je možné, v anonymizovanej forme.

4.3 Komunikácia a autentifikácia

- E-mail a telefón sú považované za dostatočne bezpečné aj bez šifrovania pri nízko citlivých údajoch.
- Pre vysoko citlivé dáta sa používa PGP.
- Autentifikácia osoby je možná prostredníctvom web of trust, spätného volania, spätného e-mailu alebo osobného stretnutia.

Služby

5.1 Incident Response

Cieľom GOV CERT SK je riešenie a koordinácia bezpečnostných incidentov. Poskytuje pomoc pri:

- nepretržitom bezpečnostnom monitoringu,
- vydávaní výstrah a upozornení,
- analýze a reakcii na incidenty,
- analýze a reakcii na artefakty,
- poskytovaní dokumentácie pre riešenie bežných incidentov,
- analýze a reakcii na zraniteľnosti,
- koordinácii riešenia incidentov pre GOVNET.

5.2 Proaktívne aktivity

GOV CERT SK koordinuje a poskytuje:

- oznámenia bezpečnostných upozornení,
- školenia a semináre pre zvyšovanie povedomia,

- koordináciu preventívnych opatrení v kyberpriestore,
- spoluprácu s príslušnými orgánmi na identifikácii hrozieb,
- proaktívne filtrovanie škodlivého obsahu a potenciálne nebezpečných zdrojov na úrovni dátovej siete.

Formulár na hlásenie incidentu

Dostupný na: https://cert.gov.sk/nahlasenie-incidentu

Vyhlásenie o zodpovednosti

Pri príprave informácií, oznámení a upozornení budú prijaté všetky opatrenia, avšak GOV CERT SK nenesie zodpovednosť za chyby, opomenutia ani škody spôsobené použitím týchto informácií.