(RFC 2350)

SIGOV-CERT RFC 2350

1 Podatki o dokumentu

Ta dokument opisuje SIGOV-CERT v skladu z RFC 2350.

1.1 Datum zadnje posodobitve

Verzija 1.0, objavljena 31. januarja 2019.

1.2 Seznam prejemnikov obvestil o spremembah

Spremembe tega dokumenta se ne razpošiljajo.

1.3 Mesto, kjer se ta dokument nahaja

Ta dokument se nahaja na spodnjem naslovu:

http://www.mju.gov.si/si/delovna_podrocja/informatika/informacijska_varnost/

Najnovejša verzija je na voljo na zahtevo preko elektronske pošte cert(at)gov.si.

2 Kontaktne informacije

2.1 Ime skupine

SIGOV-CERT: Odzivni center za incidente v informacijskih sistemih državne uprave (slovensko ime).

SIGOV-CERT: Slovenian Governmental Computer Emergency Response Team (angleško ime).

2.2 Naslov

SIGOV-CERT
Ministrstvo za javno upravo
Direktorat za informatiko
Sektor za informacijsko varnost

Tržaška c. 21,
SI-1000 Ljubljana
Slovenija

2.3 Časovni pas

- CET, Centralni evropski čas
  (UTC+1, med zadnjo nedeljo v oktobru in zadnjo nedeljo v marcu)
- CEST (tudi CET DST), Centralni evropski poletni čas
  (UTC+2, med zadnjo nedeljo v marcu in zadnjo nedeljo v oktobru)

2.4 Telefonska številka

+386 1 478 86 51

2.5 Fax

+386 1 478 86 49

2.6 Ostale telekomunikacije

Poleg telefona, faksa in e-pošte drugih telekomunikacij ni.

2.7 Naslov elektronske pošte

cert(at)gov.si

2.8 Javni ključi in informacije o šifriranju

Za digitalne podpise in za sprejemanje šifriranih informacij SIGOV-CERT uporablja PGP enkripcijo. Ključ PGP/GPG je na voljo na spletni povezavi:
http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/Direktorat_za_informatiko/sigov-cert-pgp.asc.asc

Informacije o ključu:

pub rsa4096 2019-01-24 [SCA] [expires: 2024-01-24]
Key fingerprint = 3002 991D C8A4 3CB3 2D57 16F0 EDBD E956 865C 503B
uid SIGOV-CERT <SIGOV-CERT(at)gov.si>
uid SIGOV-CERT <cert(at)gov.si>

2.9 Člani ekipe

Vodja skupine SIGOV-CERT je Damjan Križman. Popoln seznam drugih članov SIGOV-CERT ni javno dostopen. V uradnem poročilu o incidentu in korespondenci v zvezi z incidentom se člani skupine predstavljajo z njihovim polnim imenom.

2.10 Ostale informacije

Informacije skupaj z novicami in bilteni o SIGOV-CERT v slovenskem jeziku, so na voljo na http://www.mju.gov.si/si/delovna_podrocja/informatika/informacijska_varnost/.

Splošne informacije o SIGOV-CERT v angleškem jeziku so na voljo na http://www.mju.gov.si/en/areas_of_work/information_and_communications_technology/.

2.11 Stiki s strankami

Najprimernejši način vzpostavitve stika s SIGOV-CERT je po elektronski pošti na naslov cert(at)gov.si. Poslovni čas SIGOV-CERT je med ponedeljkom in petkom, med 8.00 in 16.00. V času uradnih ur je osebje SIGOV-CERT na voljo tudi preko telefona. Zunaj uradnih ur osebje redno preverja e-poštni predal cert(at)gov.si.

3 Statut

3.1 Poslanstvo

SIGOV-CERT nudi pomoč pri obravnavi incidentov informacijske varnosti ter zagotavlja koordiniranje vseh incidentov s področja informacijske varnosti, ki vključujejo sisteme in omrežja v upravljanju Direktorata za informatiko, Ministrstva za javno upravo.

SIGOV-CERT pomaga pri ozaveščanju s področja informacijske varnosti v državni upravi.

3.2 Okrožje

SIGOV-CERT je odzivni center za incidente v informacijskih sistemih državne uprave, kar vključuje vsa omrežja, informacijske sisteme in uporabnike informacijskih sistemov, ki jih upravlja Ministrstvo za javno upravo.

3.3Delovanje

SIGOV-CERT deluje znotraj Direktorata za informatiko, Sektorja za informacijsko varnost na Ministrstvu za javno upravo.

3.4 Organ

SIGOV-CERT deluje v okviru pristojnosti Ministrstva za javno upravo. SIGOV-CERT si prizadeva za ohranjanje aktivnega sodelovanja in partnerstev z vsemi slovenskimi ponudniki internetnih storitev (ISP), organi pregona in drugimi deležniki na področju varnosti omrežij in informacij.

4 Pravila

4.1 Vrste incidentov in ravni podpore

SIGOV-CERT obravnava različne vrste varnostnih incidentov, ki se pojavljajo v informacijskih sistemih in na omrežjih, ki jih upravlja Direktorat za informatiko na Ministrstvu za javno upravo. Stopnja podpore je odvisna od vrste incidenta in njegove resnosti, ki jo določi osebje SIGOV-CERT.

4.2 Sodelovanje, medsebojno izmenjevanje in razkritje informacij

SIGOV-CERT obravnava vse informacije, vključene v korespondenco kot zaupne. Informacije bodo razkrite samo tistim s potrebo po vedenju, ki sodelujejo pri reševanju in preiskavi prijavljenega incidenta. Vsi podatki, ki se nanašajo na vpletene uporabnike in niso bistveni za preiskavo, bodo anonimizirani.

SIGOV-CERT razkrije informacije drugim državnim organom samo v skladu z veljavno zakonodajo.

4.3 Komunikacija in avtentikacija

Komunikacija poteka preko elektronske pošte. SIGOV-CERT uporablja PGP ključ za podpisovanje elektronskih sporočil, z občutljivo vsebino ali pa se zahteva preverjanje pristnosti. Vse občutljive komunikacije za SIGOV-CERT je potrebno šifrirati s PGP ključem. Po telefonu se je možno dogovoriti tudi o alternativnih metodah.

5 Pomoč/podpora

5.1 Odzivi na incidente

SIGOV-CERT bo pomagal vsakomur v javni upravi pri obravnavanju incidentov informacijske varnosti skladno s 74a. členom Zakona o državni upravi. Zagotavljal bo zlasti pomoč in svetovanje v zvezi z naslednjimi vidiki upravljanja incidentov:

5.1.1. Triaža incidenta

- Preiskovanje ali je dejansko zgodil incident.
- Določanje obsega incidenta.

5.1.2. Koordinacija incidentov

- Določitev vzroka, zakaj je incident nastal.
- Obveščanje uporabnikov in skrbnikov morebitnih drugih vpletenih informacijskih sistemov.

- Poročanje drugim centrom CERT/CSIRT.
- Sestavljanje obvestil uporabnikom, kadar je to primerno in potrebno.

5.1.3. Rešitve incidentov

- Svetovanje pri odpravi ranljivosti informacijskega sistema oziroma vzpostavitvi dodatne zaščite za preprečevanje morebitnih novih incidentov.
- Ocenjevanje, kateri ukrepi so najbolj primerni za zagotavljanje želenih rezultatov v zvezi z resolucijo incidenta.
- Nudenje pomoči pri zbiranju dokazov in razlagi podatkov, kadar je to potrebno.

5.2 Proaktivne dejavnosti

- **Ozaveščanje**
  SIGOV-CERT izvaja program ozaveščanja, ki je namenjen javnim uslužbencem. Cilji programa so zagotoviti učinkovite metode za prepoznavanje tveganja in njihovo ublažitev.
- **Informacijski sistemi**
  SIGOV-CERT objavlja nasvete za dogodke in incidente, ki so posebno pomembni za uporabnike.
- **Izobraževanja**
  Člani SIGOV-CERT občasno pripravljajo in se udeležujejo predavanj, seminarjev in delavnic na temo informacijske varnosti.

6 Obrazci za poročanje o incidentih

Poročila se lahko pošilja preko elektronske pošte, na naslov cert@gov.si, za uporabnike v državnem omrežju, pa se uporablja za to namenjeno orodje ali naslov ekc(at)gov.si.

.

7 Opozorila

SIGOV-CERT ne prevzema nobene odgovornosti za napake, opustitve ali škodo, ki izhajajo iz uporabe tu pridobljenih informacij.