RFC2350

1. Informacije o dokumentu

Ovaj dokument sadrži informacije o OITeG CERT-u.

1.1. Datum poslednje izmene

17.06.2023.

1.2. Distribucijska lista za obaveštenja

Ne postoji distribucijska lista za obaveštavanje o izmenama u ovom dokumentu.

1.3. Mesta na kojima je ovaj dokument dostupan

Poslednja verzija ovog dokumenta se nalazi na : https://www.ite.gov.rs/tekst/sr/88/cert.php

2. Kontaktne informacije

2.1. Ime CSIRT tima

OITeG CERT (Office for IT and eGovernment Computer Emergency Response Team)

2.2. Adresa

Nemanjina 11, Beograd, 11000, Srbija

2.3. Vremenska zona

CET; UTC+01:00

2.4. Broj telefona

+ 381 11 7358 400

2.5. Broj faksimila

/

2.6. Druge metode kontakta

Ne postoje

2.7. Adresa Elektronske pošte

cert@gov.rs

2.8. Javni ključevi i informacije za enkripciju

Key Fingerprint= 27669C7FFC5B64396F84E47418244C141B54747D

2.9. Članovi tima

Članovi OITeG CERT-a će se identifikovati po stupanju u komunikaciju.

2.10. Druge informacije

Sve informacije o OITeG CERT-u su dostupne na: https://www.ite.gov.rs/tekst/sr/88/cert.php

2.11. Preferirane metode komunikacije

Primarni metod komunikacije je korišćenjem email-a preko cert@gov.rs, a sekundarni metod je putem telefona +381 11 7358 400

3. Povelja

3.1. Misija

Glavni zadatak CERT-a republičkih organa je da obezbeđuje informacionu bezbednost IKT infrastrukture, usluga Kancelarije i jedinstvene informaciono-komunikacione mreže elektronske uprave. Ovo uključuje efikasno reagovanje i rešavanje incidenata kada do njih dođe, preventivne aktivnosti kako bi se broj mogućih incidenata minimizovao i podizanje svesti IKT bezbednosti kod državnih organa.

3.2. Konstituenti

CERT republičkih organa obavlja poslove koji se odnose na zaštitu od incidenata u sistemima republičkih organa u jedinstvenoj informaciono-komunikacionoj mreži elektronske uprave.

3.3. Sponzorstvo ili pripadnost

OITeG CERT se nalazi u okviru Kancelarije za informacione tehnologije i elektronsku upravu nadležne za projektovanje, razvoj, izgradnju, održavanje i unapređenje jedinstvene informaciono-komunikacione mreže elektronske uprave.

3.4. Nadležnost

Centar za bezbednost informaciono-komunikacionih sistema organa (CERT republičkih organa) osnovan je (Zakon o informacionoj bezbednosti, ''Službeni glasnik Republike Srbije'', broj 6/2016 i 94/2017) u okviru Kancelarije za informacione tehnologije i elektronsku upravu nadležne za projektovanje, razvoj, izgradnju, održavanje i unapređenje jedinstvene informaciono-komunikacione mreže elektronske uprave (Zakon o elektronskoj upravi, ''Službeni glasnik Republike Srbije'', broj 27/2018).

4. Politike

4.1. Vrste incidenata i nivo podrške

Pri odgovoru na incidente OITeG CERT odgovara na sve vrste incidenata te ima koordinatorsku ulogu kako bi izvršio one aktivnosti koje su potrebne da bi se donele ispravne odluke od detekcije pa do razrešenja incidenta. Sve ostale usluge kao što su otkrivanje ranjivosti, monitoring i detekcija od strane SOC tima, koordinacija sa drugim organizacijama i obaveštavanje i edukacija OITeG CERT izvršava u potpunosti u svrhu zaštite i unapređenja bezbednosti sistema državnih institucija i organizacija.

4.2. Saradnja, interakcija i deljenje informacija

OITeG CERT pridaje veliku pažnju privatnosti tako da će svi deljeni podaci biti deljeni bez ličnih ili osetljivih podataka. Podaci koji mogu biti deljeni od strane OITeG CERT-a su statistički.

Za svaku razmenu informacija OITeG CERT koristi TLPv2. Više informacija o načinu na koji se TLPv2 koristi na https://www.ite.gov.rs/extfile/sr/6981/TLP.docx

4.3. Komunikacija i autentikacija

OITeG CERT svu komunikaciju smatra poverljivom. Gde god se dele osetljivi podaci putem email-a trebalo bi koristiti PGP/GPG, dok informacije koje nisu osetljive mogu da se dele bez enkripcije.

Telefonska komunikacija se smatra bezbednom za deljenje svih informacija.

5. Usluge

5.1. Reaktivne usluge

- reagovanje na sigurnosne incidente;
- reagovanje na sigurnosne ranjivosti i propuste;
- upozorenja o uočenim incidentima i ranjivostima.

5.2. Proaktivne usluge

- praćenje korišćenih tehnologija;
- sprovođenje bezbednosne revizije i procene sistema i usluga Kancelarije;
- konfigurisanje i održavanje sigurnosnih alata;
- detektovanje upada u sistem;
- objavljivanje novih informacija i vesti od značaja za informacionu bezbednost;
- diseminaciju znanja državnim organima u vezi sa informacionom bezbednošću;
- sprovođenje bezbednosne revizije i procene.

5.3. Usluge u domenu upravljanja kvalitetom bezbednosti

- analiza rizika;
- obezbeđivanje kontinuiranog poslovanja u situacijama kada dođe do incidenata;
- podizanje nivoa svesti o informacionoj bezbednosti;
- edukaciju zaposlenih.

6. Forma za prijavu incidenta

Forma za prijavu incidenta se nalazi na https://www.ite.gov.rs/tekst/sr/88/cert.php

7. Izjava odricanja od odgovornosti

OITeG CERT preduzima sve korake kako bi osigurao ispravnost informacija koje deli, ali ne preuzima odgovornost za bilo kakvu štetu nastalu korišćenjem istih.