**RFC 2350**

1. Informacije o dokumentu
   Ovaj dokument pruža opis MUP CERT-a u skladu sa RFC 2350.

   1.1. Datum poslednje izmene dokumenta
   Verzija 1.0 – 2018/07/12.

   1.2. Lista za distribuciju obaveštenja
   Nije dostupna.

   1.3. Lokacija na kojoj se može doći do dokumenta
   Tekuća verzija dolumenta u kojoj se opisuje MUP CERT se može naći na veb sajtu Ministarstva unutrašnjih poslova www.mup.gov.rs.

2. Kontakt

   2.1. Ime tima
   (engleski)Center for Emergency Response in Targeting ICT systems of Ministry of Interior of Republic of Serbia (srpski) Centar za reagovanje na napade na informacioni sistem skraćeno ime tima: MUP CERT

   2.2. Adresa
   Kneza Miloša 101, 11000 Beograd, Srbija

   2.3. Vremenska zona
   CET

   2.4 Broj telefona
   +381 11 361 7814

   2.5 Faks
   N/A

   2.6 Elektronska pošta
   Sve zahteve (uključujući i zahteve u vezi incidenata) treba uputiti na: cert@mup.gov.rs

   2.7 Ostali vidovi komunikacije
   N/A

   2.8 Informacije o tipu enkripcije i javnom ključu
   Za funkcionalnu razmenu informacija između MUP CERT-a i partnera (izveštavanje o incidentima, upozorenja...) koristi se PGP.
   Key ID: D29C2FDB
   Fingerprint: 5700 91DA E841 5DF7 DFE7 561F 7B32 15C7 D29C 2FDB

   2.9 Članovi tima
   Imena članova tima nisu javno dostupna. Članovi tima će se identifikovati punim imenom u zvaničnoj komunikaciji sa stranom koja prijavljuje incident.

2.10 Ostale informacije

2.11 Način komunikacije sa korisnicima

Poželjan metod komunikacije sa MUP CERT-om je elektronskom poštom. Adresu cert@mup.gov.rs monitoriše dežurni CERT-a 24/7.
Hitni slučajevi se mogu prijaviti telefonom +381 11 361 7814, 24/7
Radno vreme: ponedeljak – petak od 07.30 do 15.30
U hitnim slučajevima se radi i van radnog vremena.

3. Povelja

3.1 Misija

Misija MUP CERT-a je da podrži i zaštiti IKT sisteme Ministarstva unutrašnjih poslova sa ciljem da podaci o ličnosti, kao i ostali osetljivi podaci koji se pohranjeni u bazama podataka ministarstva ostanu poverljivi i pouzdani. Opseg aktivnosti MUP CERT-a obuhvata prevenciju, detekciju, odgovor i oporavak u slučajevima namernog i zlonamernog napada, kao i u slučajevima nenamernih postupaka koji mogu ugroziti integritet IKT sistema MUP-a i naneti štetu interesima građana R Srbije.
U slučaju potrebe MUP CERT je spreman da služi kao rezerva Nacionalnom CERT-u R. Srbije.

3.4 Nadležnost

MUP CERT je nadležan za zaposlene i IKT sisteme Ministarstva unutrašnjih poslova.

3.5 Pripadnost

MUP CERT je deo Ministarstva unutrašnjih poslova.

3.6 Ovlašćenja

Uspostavljanje MUP CERT-a je propisano Zakonom o informacionoj bezbednosti i Pravilnikom o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova.

4. Politika rada

4.1 Tipovi incidenata i nivo podrške

MUP CERT je ovlašćen da odredi i učestvuje u potpunom rešavanju svih tipova bezbednosnih računarskih incidenata koji se tiču IKT sistema MUP-a.

4.2 Saradnja, zajedničko delovanje i odnos prema dobijenim informacijama

MUP CERT pridaje veliku važnost operativnoj saradnji i razmeni informacijakako sa CERT timovima, tako i sa ostalim organizacijama koje mogu doprineti boljem nivou sajber bezbednosti.
MUP CERT sve dobijene informacije tretira kao poverljive. Dobijena informacija se može podeliti sa trećom stranom samo ukoliko je treća strana uključena u istragu ili razrešenje prijavljenog incidenta.
MUP CERT funkcioniše u okviru zakona R. Srbije.

4.3 Komunikacija i potvrda identiteta

Elektronska pošta i telefoni se smatraju za dovoljno bezbedan način komunikacije za slanje podataka koji se ne smatraju posebno osetljivim. U slučaju slanja ostljivih podataka elektronskom poštom, koristiće se PGP.

Ukoliko je neophodno da se potvrdi identitet osobe koja prijavljuje incident, to se može uraditi pomoću mreža poverenja (npr. Trusted introducer, FIRST) ili preko povratnog telefonskog poziva ili elektronske pošte.

5. Servisi

5.1 Odgovor na incident

MUP CERT asistira mrežnim i bezbednosnim administratorima MUP-a prilikom obrade tehničkih ili operativnih aspekata incidenta.

*5.1.1. Trijaža incidenata*

Utvrđivanje opsega incidenta, prioriteta i mogućeg uticaja;
Utvrđivanje početnih resursa neophodnih za rešavanje problema.

*5.1.2. Koordinacija incidenta*

Angažuje sve unutrašnje resurse potrebne za istragu incidenta i preduzima potrebne mere;
Kontaktira treću stranu koja može pomoći u razrešenju incidenta;
Kontaktira treću stranu koja može biti ugrožena incidentom.

*5.1.3. Rešavanje incidenta*

Pruža savete mrežnim i sistemskim administratorima po pitanju mera koje je potrebno preduzeti;
Pruža pomoć u prikupljanju dokaza i tumačenju (tehničkih) informacija;
Ukoliko je potrebno, MUP CERT izlazi na lice mesta u cilju razrešenja problema.

5.2 Proaktivne aktivnosti

MUP CERT pruža obaveštenja i upozorenja iz svoje nadležnosti zaposlenima i sistem administratorima MUP-a, kao i ostalim CERT timovima u zemlji.
MUP CERT je uključen u podizanje bezbednosne svesti svih zaposlenih u MUP-u.

6. Obrazac za prijavu incidenta

Molimo navedite MUP CERT-u minimalno sledeće informacije:

- kontakt podatke – ime i prezime osobe koja prijavljuje incident i/ili ime i adresu organizacije koja prijavljuje incident, adresu elektronske pošte, broj telefona;
- IP adresu i zapažanja.

7. Odricanje od odgovornosti

Iako će svaka mera predostrožnosti biti preduzeta u pripremi informacija, obaveštenja i upozorenja, MUP CERT ne preuzima odgovornost za greške ili propuste, ili za štete nastale korišćenjem sadržanih informacija.