



13. oktober 2025
Brdo pri Kranju

PRIJAVA INCIDENTA

Miklavž Šef
Skupina CSIRT, SIGOV-CERT, URSIV



REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

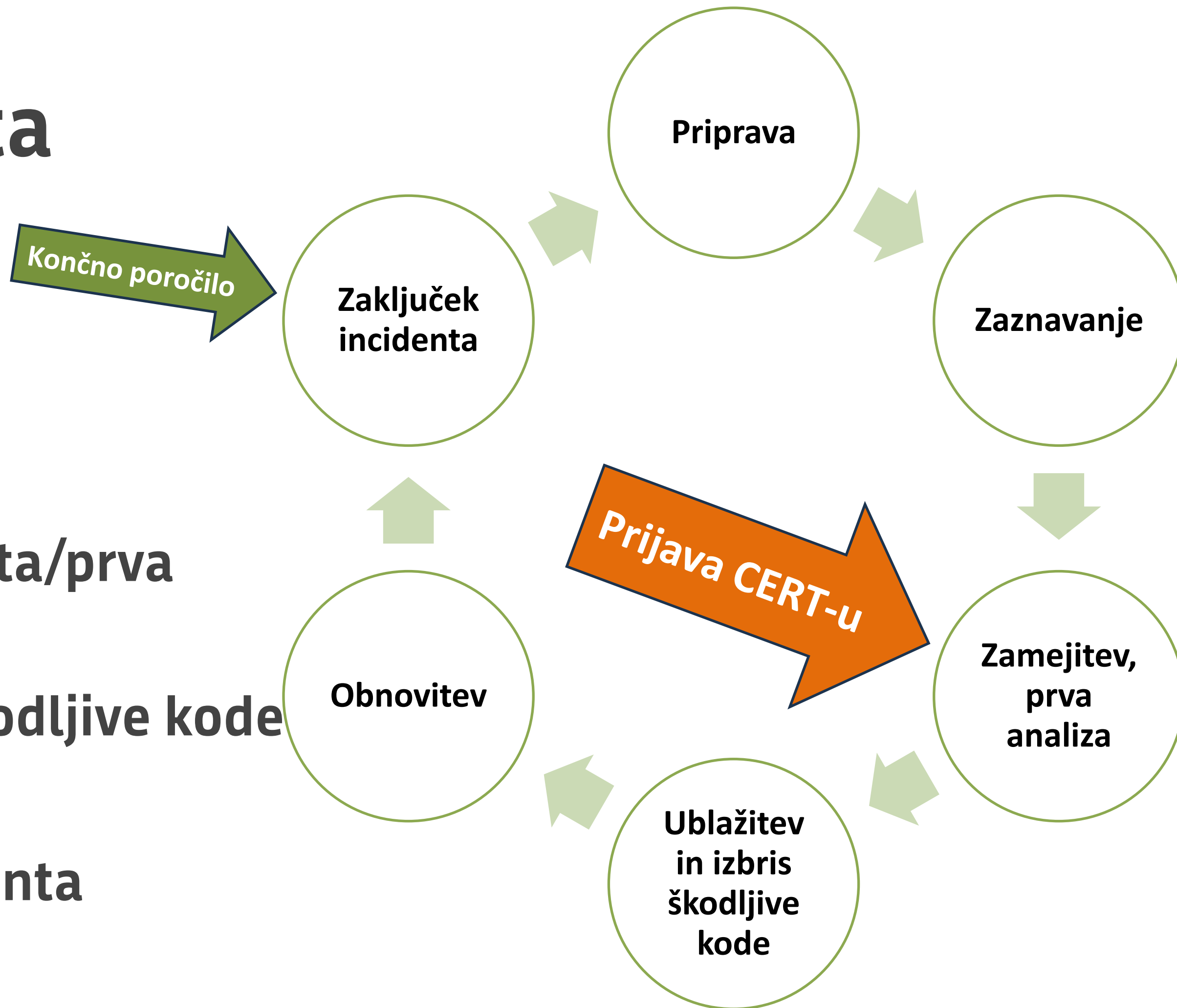
KONFERENCA ZInfV-1 ZAKON ZA KIBERNETSKO VARNO PRIHODNOST SLOVENIJE

Pomembni incident

- **Povzroči ali bi lahko povzročil:**
 - resne operativne motnje pri opravljanju storitev,
 - finančne izgube,
 - vpliv na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.
- **Bistveni in pomembni subjekti morajo pristojni skupini CSIRT **nemudoma priglasiti** vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev.**

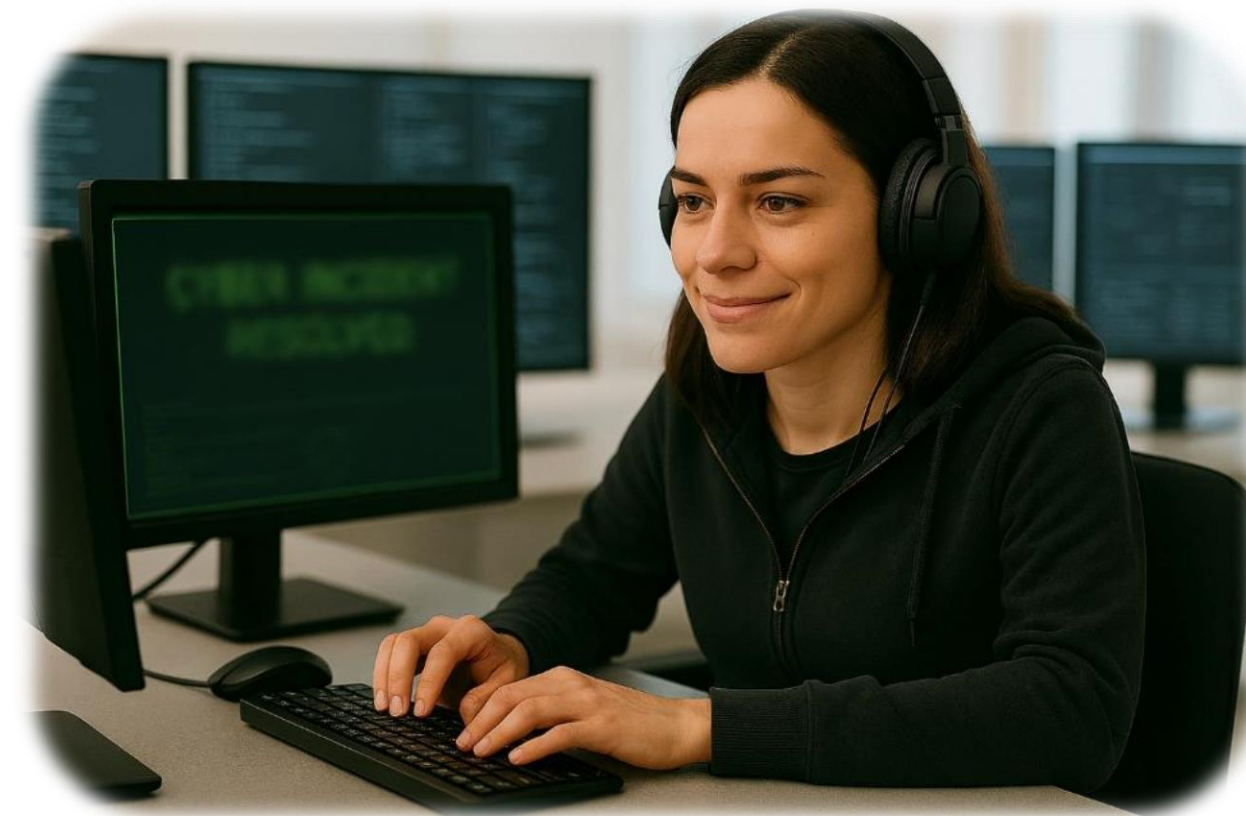
Potek incidenta

- Priprava
- Zaznavanje
- Zamejitev/zajezitev – identifikacija incidenta/prva analiza
- Ublažitev in izbris škodljive kode
- Obnovitev/okrevanje
- Faza zaključka incidenta



Kako prijaviti incident?

- E-pošta
- telefonsko
- spletni obrazec (v pripravi)
- pristojnemu CERT-u



JAVNA UPRAVA (SIGOV-CERT)
cert@gov.si

Kaj naj vsebuje prijava? 1/2

- **Kontakt**
- **Čas zaznave**
- **Opis**
- **Stopnja incidenta C1 - C6 (določi CSIRT)**
- **Vpliv na delovanje storitev**
- **Ocena vpliva (medpodročni in čezmejni)**



Kaj naj vsebuje prijava? 2/2

- Po potrebi TLP
- **Indikatorje zlorabe** (škodljiva koda, IP, domene, ...) dnevniske zapise, artefakti, ...
- **Šifriranje vsebine** (PGP, ZIP, ...)
- **Možnost odlaganja večjih datotek** (SOVD, Arnes Filesender)
- **Podatki v strojno berljivi obliki**
(csv json xml log evt)



Časovni roki za obvezno poročanje

- **V 24. urah:**
zgodnje sporočilo o zaznavi pomembnega incidenta
- **V 72. urah:**
priglasitev incidenta (trenutno obrazec Priloga E iz NOKI)
- **Vmesna poročila po potrebi.**
- **Končno poročilo najpozneje v enem mesecu po priglasitvi incidenta, oziroma najpozneje mesec po rešitvi incidenta.**



POMEMBNO



- **Prijava CERTu ne pomeni avtomatičnega posredovanja informacij inšpekcijam.**
- **Prijave obravnavamo z visoko mero zaupanja.**
- **S prijavo pomagajte sebi in drugim.**

Kontakti za prigrasitev

JAVNA UPRAVA (SIGOV-CERT)

cert@gov.si

OSTALI (SI-CERT)

cert@cert.si



REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

HVALA ZA POZORNOST

Miklavž Šef
cert@gov.si



URSIV
KIBERNETSKO VARNI

KONFERENCA ZInfV-1
Zakon za kibernetско
varno prihodnost Slovenije