PLATFORMA PIXI

NKS KONFERENCIJA, 28.05.2025

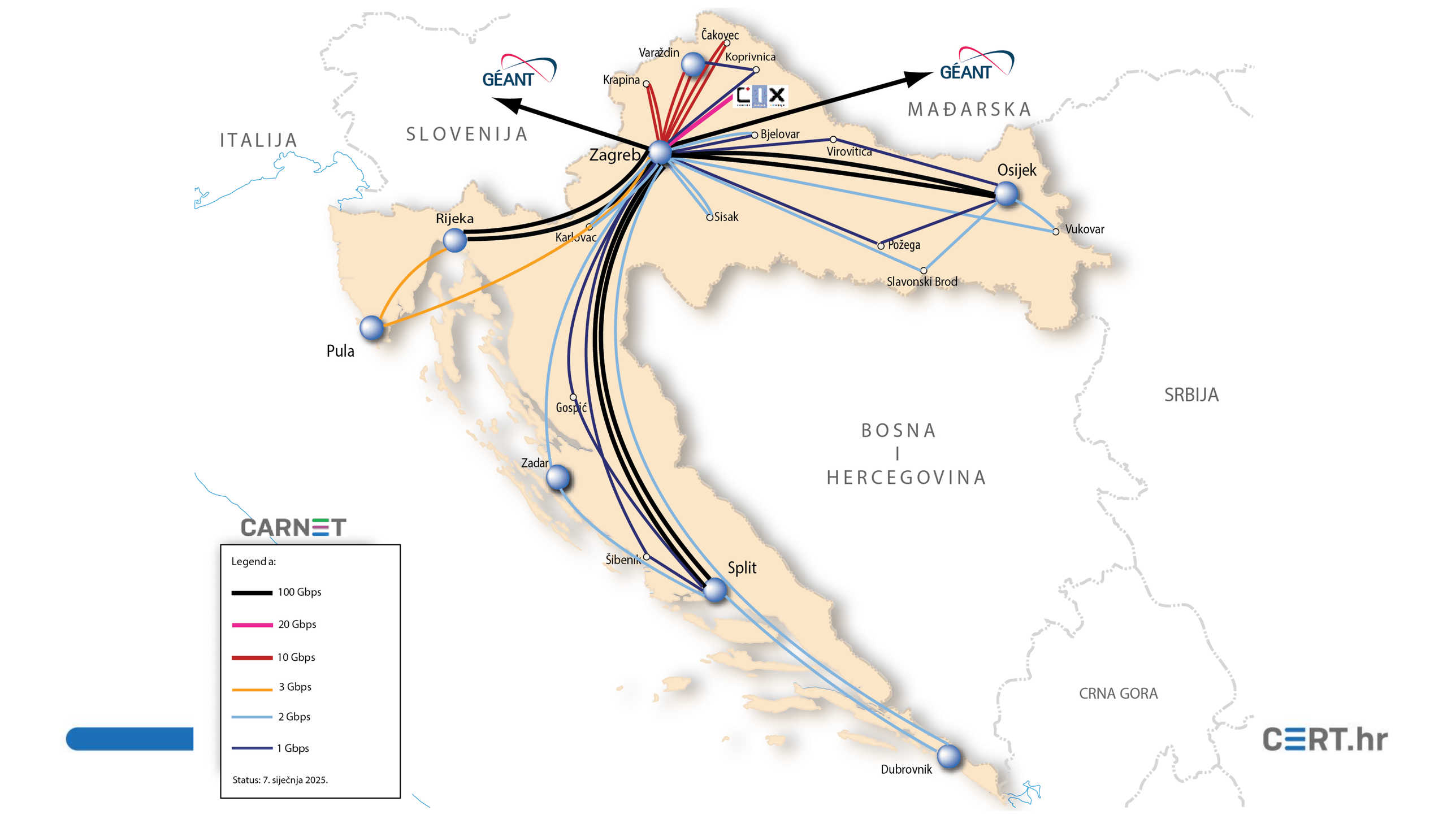
Nataša Glavor

Pomoćnica ravnatelja CARNET-a za Nacionalni CERT

CERT.hr

Kratko o CARNET-u

- Hrvatska akademska i istraživačka mreža
- Javna ustanova koje djeluje u sklopu Ministarstva znanosti, obrazovanja i mladih
- Osnovana 1991. najprije kao projekt tadašnjeg Ministarstva znanosti i tehnologije i postaje prvi pružatelj usluga pristupa Internetu u RH
- CARNET mreža je privatna mreža akademske i istraživačke zajednice RH, kao i institucija iz obrazovnog sustava
- Na CARNET mrežu spojeno je preko 3000 lokacija ustanova iz sustava znanosti, akademske i obrazovne zajednice


GÉANT
GÉANT
Čakovec
Varaždin
Koprivnica
Krapina
MAĐARSKA
ITALIJA
SLOVENIJA
Bjelovar
Virovitica
Zagreb
Osijek
Rijeka
Sisak
Vukovar
Karlovac
Požega
Slavonski Brod
Pula
Gospić
SRBIJA
BOSNA
I
HERCEGOVINA
Zadar
CARNET
Šibenik
Split
Legend a:
100 Gbps
20 Gbps
10 Gbps
3 Gbps
2 Gbps
1 Gbps
Status: 7. siječnja 2025.
CRNA GORA
Dubrovnik
CERT.hr

Kratko o CERT.hr

- Osnovan Zakonom o informacijskoj sigurnosti kao tijelo zaduženo za prevenciju i zaštitu od kibernetičkih prijetnji javnih informacijskih servisa u Republici Hrvatskoj
- Organizacijska jedinica Hrvatske akademske i istraživačke mreže – CARNET
- Prema Zakonu o kibernetičkoj sigurnosti nadležni smo CSIRT za nekoliko sektora

Uloga nacionalnog CERT-a

- Osnovna zadaća – zaštita i prevencija od kibernetičkih prijetnji
  - javnih subjekata
  - privatnih subjekata
  - akademske i obrazovne zajednice
  - građana
- Koordinacija i pomoć pri rješavanju kibernetičkih incidenata kad je jedna od uključenih strana iz hrvatskog IP adresnog ili domenskog prostora
  - osim državnih tijela, pravnih osoba s javnim ovlastima i jedinica lokalne i područne (regionalne) samouprave -> nadležnost NCSC-a

Uloge CARNET-a i Nacionalnog CERT-a u provedbi NIS2 Direktive

Nadležni CSIRT za 4+ sektora

Razvoj, prilagodba i upravljanje PiXi platformom

Uloga nadležnog CSIRT-a

- prati kibernetičke prijetnje i ranjivosti, pruža rano upozorenje ključnim i važnim subjektima
- na zahtjev, može pomoći subjektima u praćenju njihovog stanja kibernetičke sigurnosti, može proaktivno skenirati uređaje spojene na Internet kako bi otkrio ranjivosti s potencijalno značajnim utjecajem
- prima i obrađuje značajne kibernetičke incidente
- ako je potrebno, pruža informacije u vezi s daljnjim djelovanjem, posebno onima koje mogu doprinijeti učinkovitom rješavanju značajnog incidenta
- surađuje na nacionalnoj i međunarodnoj razini s drugim CSIRT timovima, razmjenjuje informacije, pruža uzajamnu pomoć

Nadležni CSIRT za sektore NIS2

Što je Platforma PiXi?

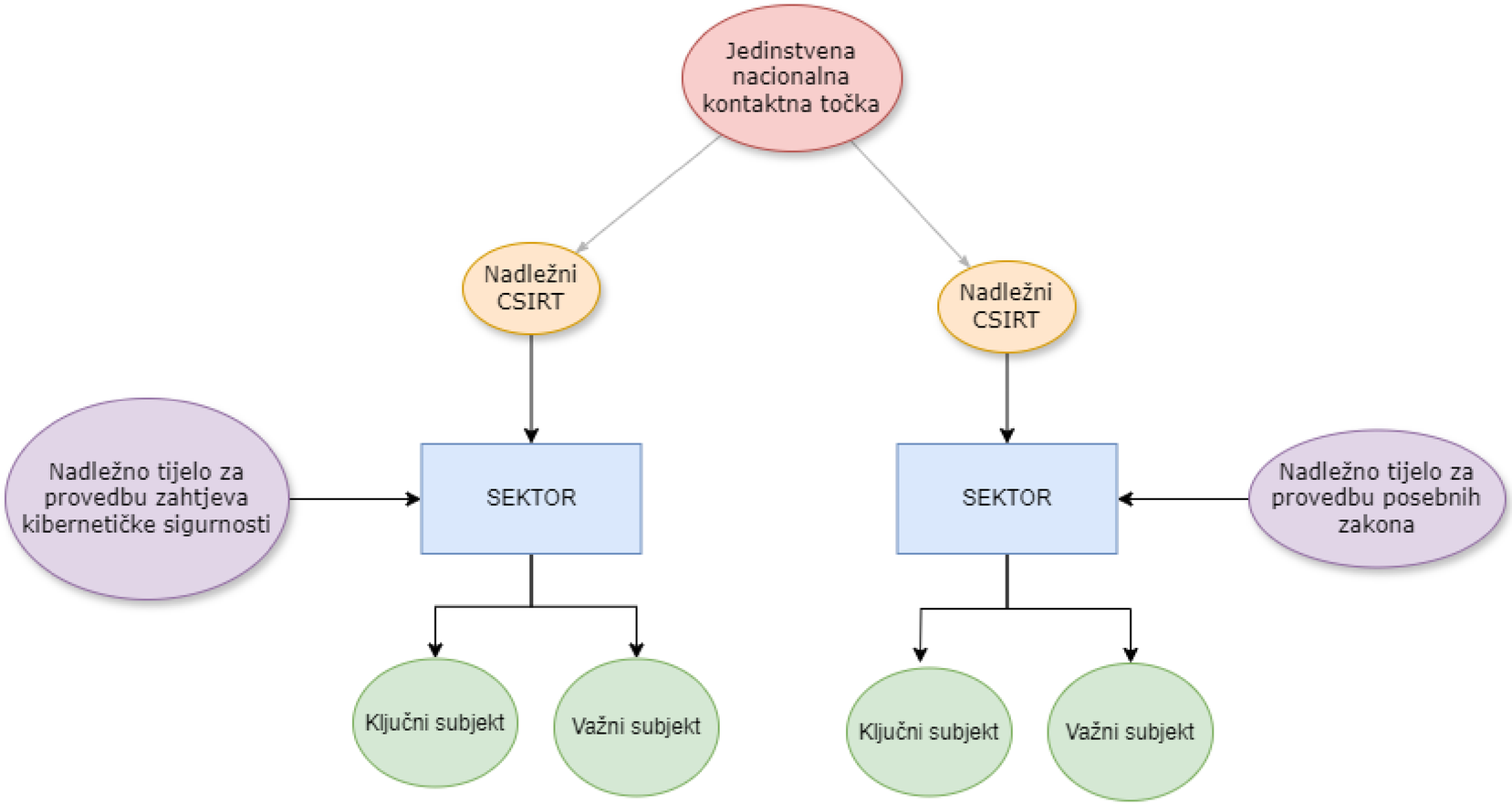
- Nacionalna platforma za izvještavanje o značajnim incidentima prema Zakonu o kibernetičkoj sigunosti i Zakonu o provedbi Uredbe Dora, izvještavanje i razmjenu informacija o ostalim incidentima, izbjegnutim incidentima i prijetnjama

  - Članak 43. – Obavještavanje i razmjena podataka o kibernetičkim prijetnjama i incidentima među nadležnim tijelima provodi se putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, kao jedinstvene ulazne točke za obavješćivanje o kibernetičkim prijetnjama i incidentima

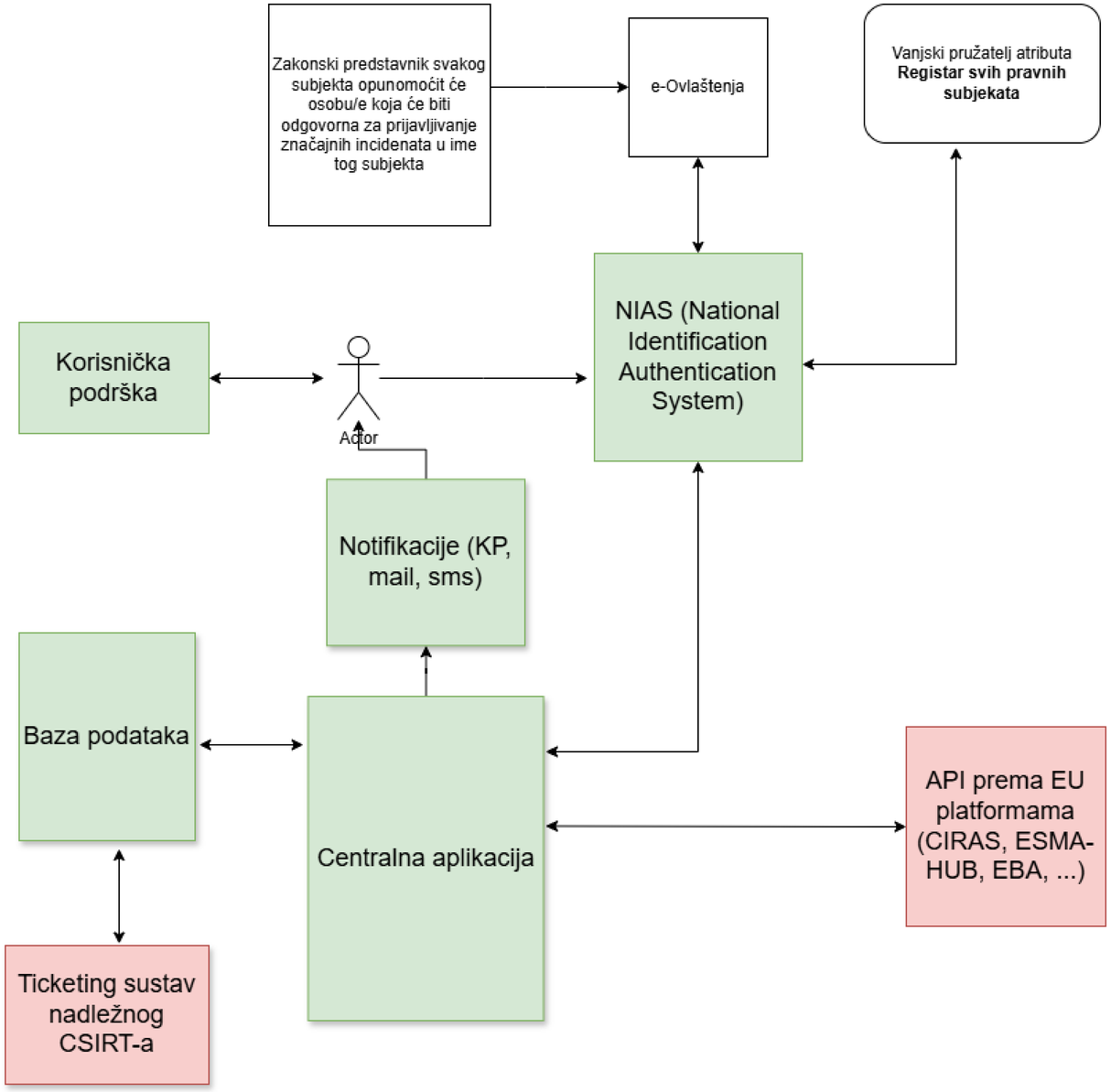
Korisnici Platforme PiXi

- PiXi platforma prilagođena potrebama NIS2 direktive zatvoren je sustav kojem pristup imaju:
  - ključni i važni subjekti,
  - nadležni CSIRT-ovi,
  - nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti,
  - nadležna tijela za provedbu posebnih zakona,
  - jedinstvena kontaktna točka

Uloge u Platformi PiXi

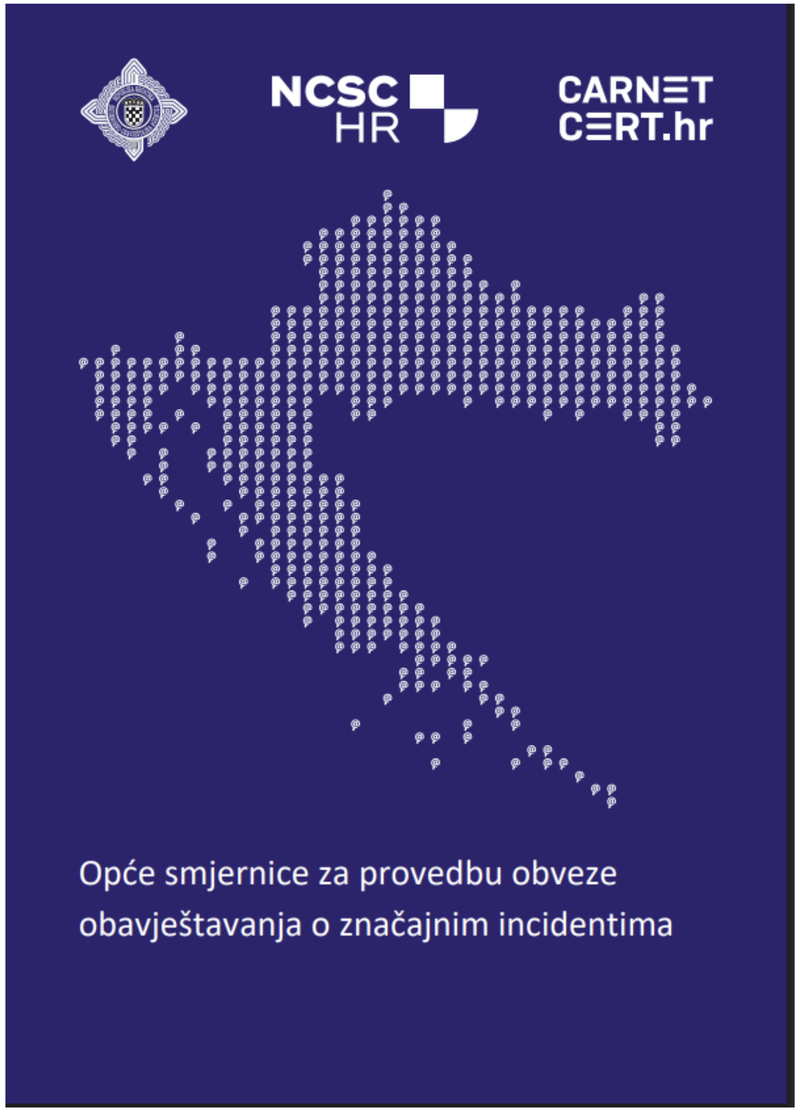


Arhitektura Platforme PiXi

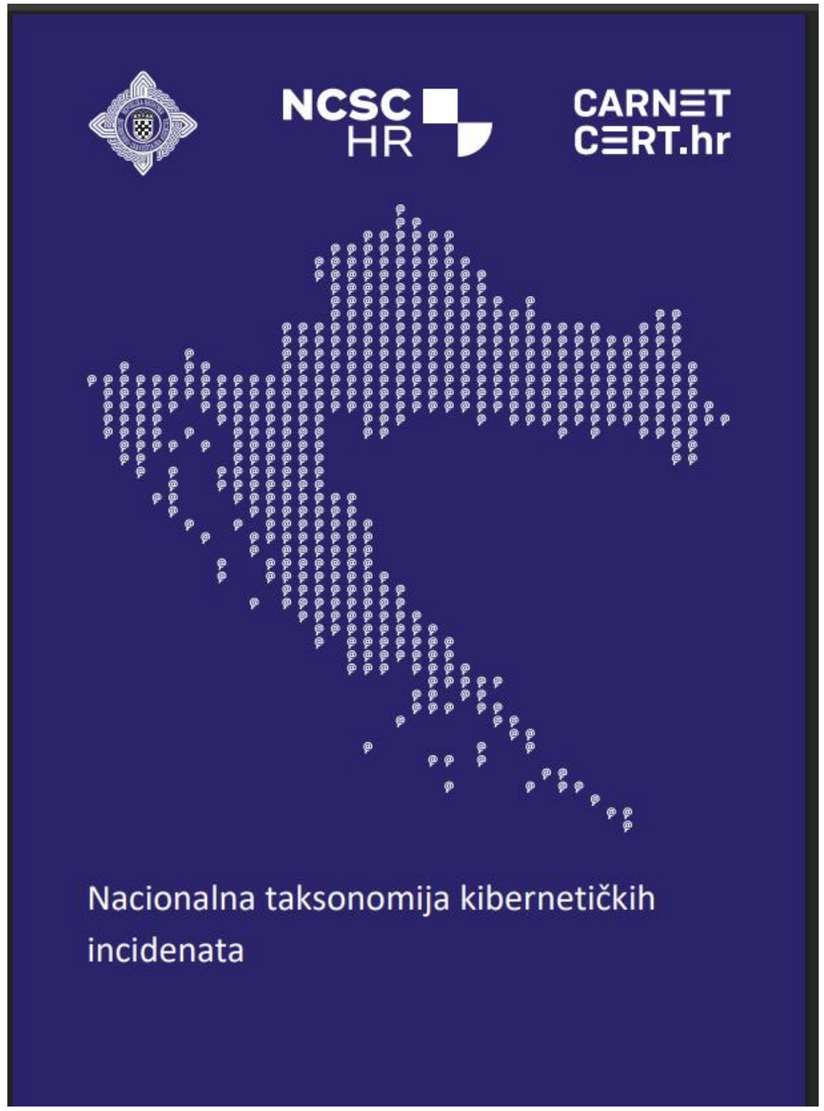


Obavještavanje prema ZKS-u kroz PiXi

- Značajni incidenti:
  - Rano upozorenje
  - Početnu obavijest
  - (Privremeno izvješće)
  - (Izvješće o napretku)
  - Završno izvješće
- Ostali incidenti
- Izbjegnuti incidenti
- Prijetnje

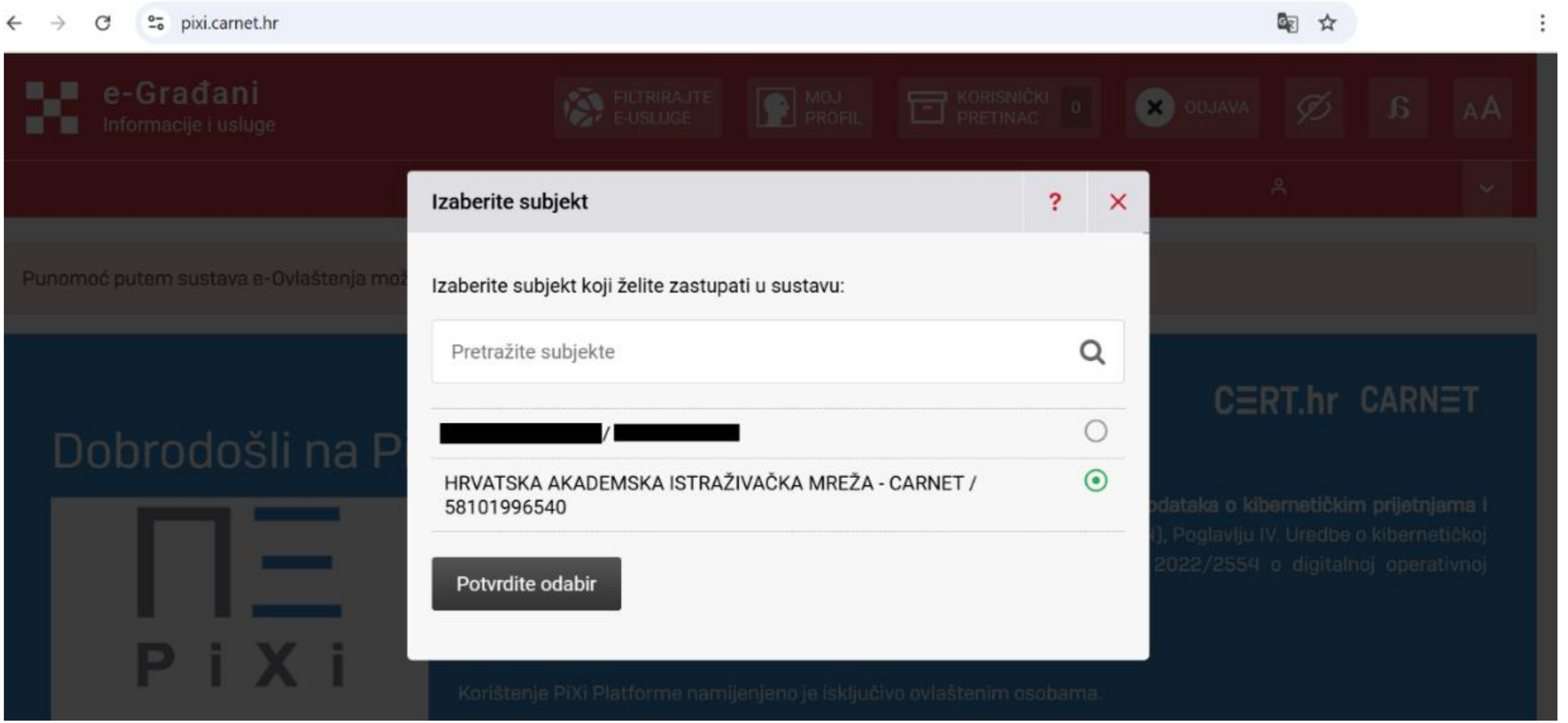


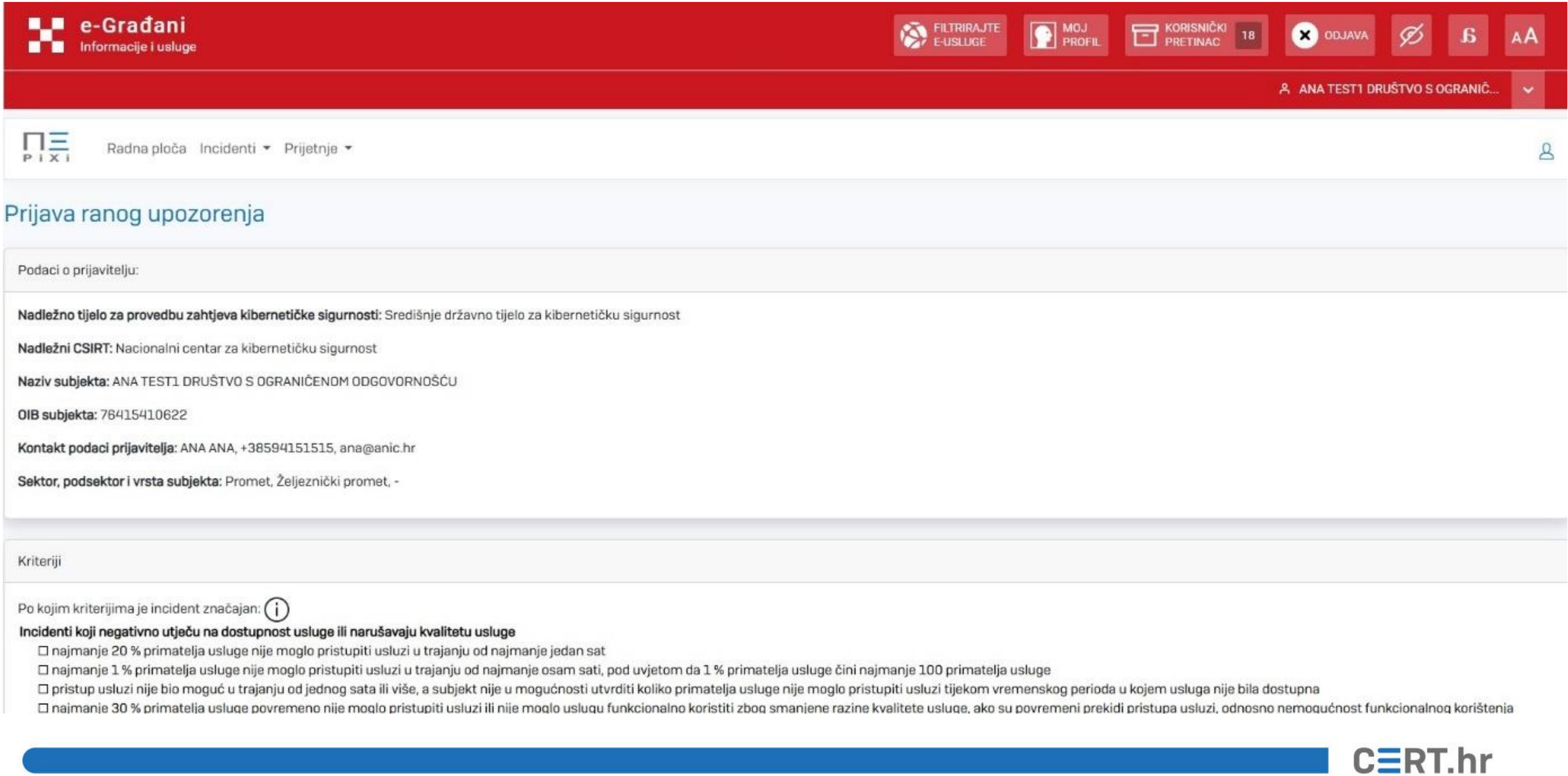
- Opće smjernice za provedbu obveze obavještavanja o značajnim incidentima dostupne na poveznicama:
- https://www.cert.hr/zks-incident
- https://ncsc.hr/hr/prijava-incidenta

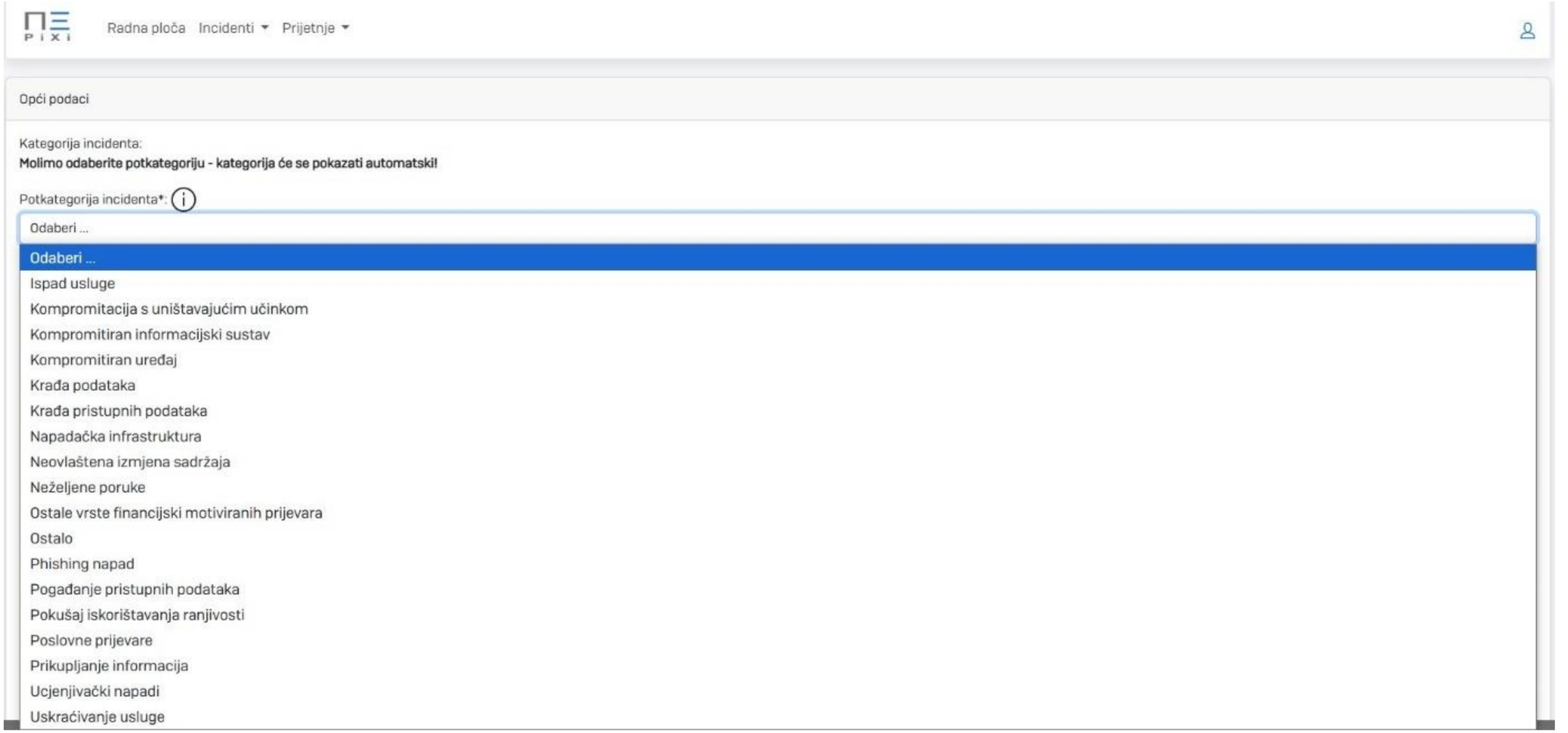


- Nacionalna taksonomija kibernetičkih incidenata dostupna na poveznicama:
- https://www.cert.hr/nacionalna-taksonomija-incidenata/
- https://ncsc.hr/hr/nacionalna-taksonomija-kibernetickih-incidenata

https://pixi.carnet.hr


pixi.carnet.hr
e-Građani
Informacije i usluge
FILTRIRAJTE E-USLUGE
MOJ PROFIL
KORISNIČKI PRETINAC
0
ODJAVA
AA
Punomoć putem sustava e-Ovlaštenja mož
Izaberite subjekt
Izaberite subjekt koji želite zastupati u sustavu:
Pretražite subjekte
[redacted]/[redacted]
HRVATSKA AKADEMSKA ISTRAŽIVAČKA MREŽA - CARNET / 58101996540
Potvrdite odabir
Dobrodošli na P
PiXi
CERT.hr CARNET
odataka o kibernetičkim prijetnjama i
), Poglavlju IV. Uredbe o kibernetičkoj
2022/2554 o digitalnoj operativnoj
Korištenje PiXi Platforme namijenjeno je isključivo ovlaštenim osobama.


e-Građani
Informacije i usluge
FILTRIRAJTE E-USLUGE
MOJ PROFIL
KORISNIČKI PRETINAC 18
ODJAVA
ANA TEST1 DRUŠTVO S OGRANIČ...
PIXI
Radna ploča
Incidenti
Prijetnje
Prijava ranog upozorenja
Podaci o prijavitelju:
Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti: Središnje državno tijelo za kibernetičku sigurnost
Nadležni CSIRT: Nacionalni centar za kibernetičku sigurnost
Naziv subjekta: ANA TEST1 DRUŠTVO S OGRANIČENOM ODGOVORNOŠĆU
OIB subjekta: 76415410622
Kontakt podaci prijavitelja: ANA ANA, +38594151515, ana@anic.hr
Sektor, podsektor i vrsta subjekta: Promet, Željeznički promet, -
Kriteriji
Po kojim kriterijima je incident značajan:
Incidenti koji negativno utječu na dostupnost usluge ili narušavaju kvalitetu usluge
☐ najmanje 20 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje jedan sat
☐ najmanje 1 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje osam sati, pod uvjetom da 1 % primatelja usluge čini najmanje 100 primatelja usluge
☐ pristup usluzi nije bio moguć u trajanju od jednog sata ili više, a subjekt nije u mogućnosti utvrditi koliko primatelja usluge nije moglo pristupiti usluzi tijekom vremenskog perioda u kojem usluga nije bila dostupna
☐ najmanje 30 % primatelja usluge povremeno nije moglo pristupiti usluzi ili nije moglo uslugu funkcionalno koristiti zbog smanjene razine kvalitete usluge, ako su povremeni prekidi pristupa usluzi, odnosno nemogućnost funkcionalnog korištenja


Radna ploča
Incidenti
Prijetnje
Opći podaci
Kategorija incidenta:
Molimo odaberite potkategoriju - kategorija će se pokazati automatski!
Potkategorija incidenta*:
Odaberi ...
Odaberi ...
Ispad usluge
Kompromitacija s uništavajućim učinkom
Kompromitiran informacijski sustav
Kompromitiran uređaj
Krađa podataka
Krađa pristupnih podataka
Napadačka infrastruktura
Neovlaštena izmjena sadržaja
Neželjene poruke
Ostale vrste financijski motiviranih prijevara
Ostalo
Phishing napad
Pogađanje pristupnih podataka
Pokušaj iskorištavanja ranjivosti
Poslovne prijevare
Prikupljanje informacija
Ucjenjivački napadi
Uskraćivanje usluge

Radna ploča Incidenti Prijetnje

Opći podaci

Kategorija incidenta:
Uspješno ostvarena kompromitacija

Potkategorija incidenta*:

Krađa podataka

Datum i vrijeme kada je otkriveno da se radi o značajnom incidentu*: DD-MM-YYYY HH:MM

Datum i vrijeme kada je incident detektiran/otkriven*: DD-MM-YYYY HH:MM

Datum i vrijeme kada je incident nastao: DD-MM-YYYY HH:MM

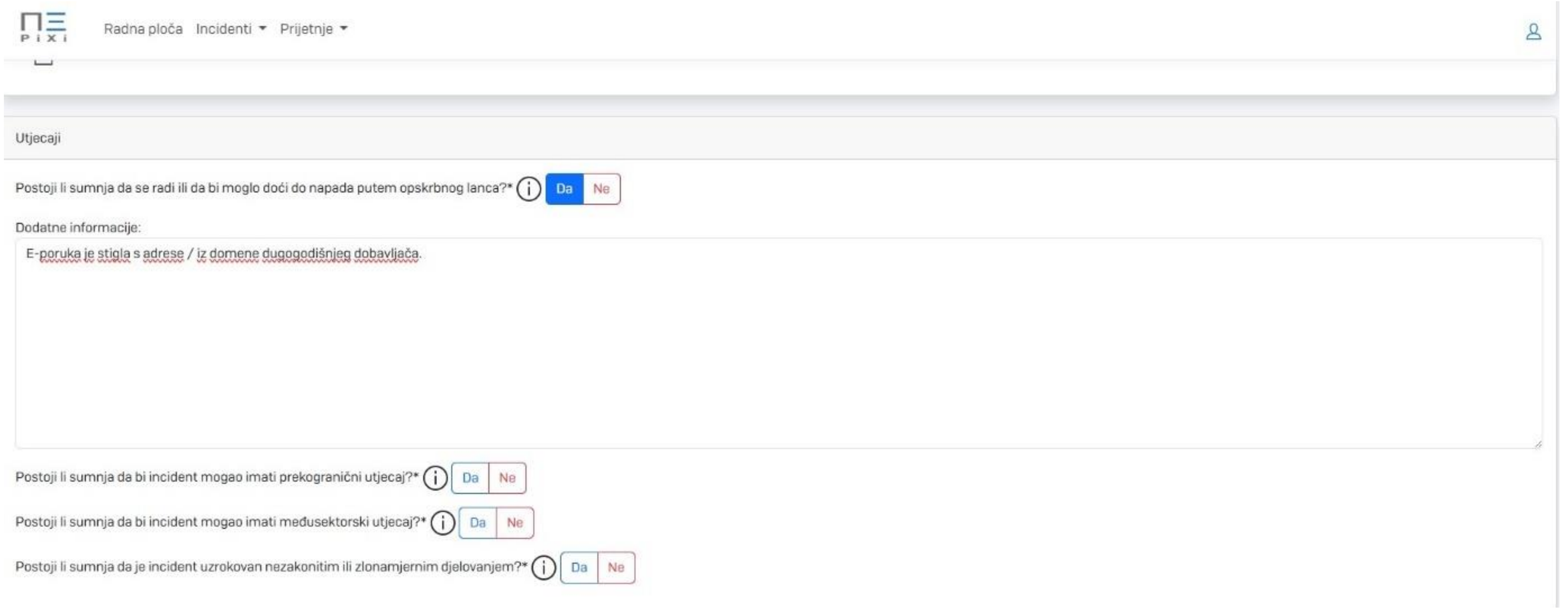
Sažetak incidenta*:

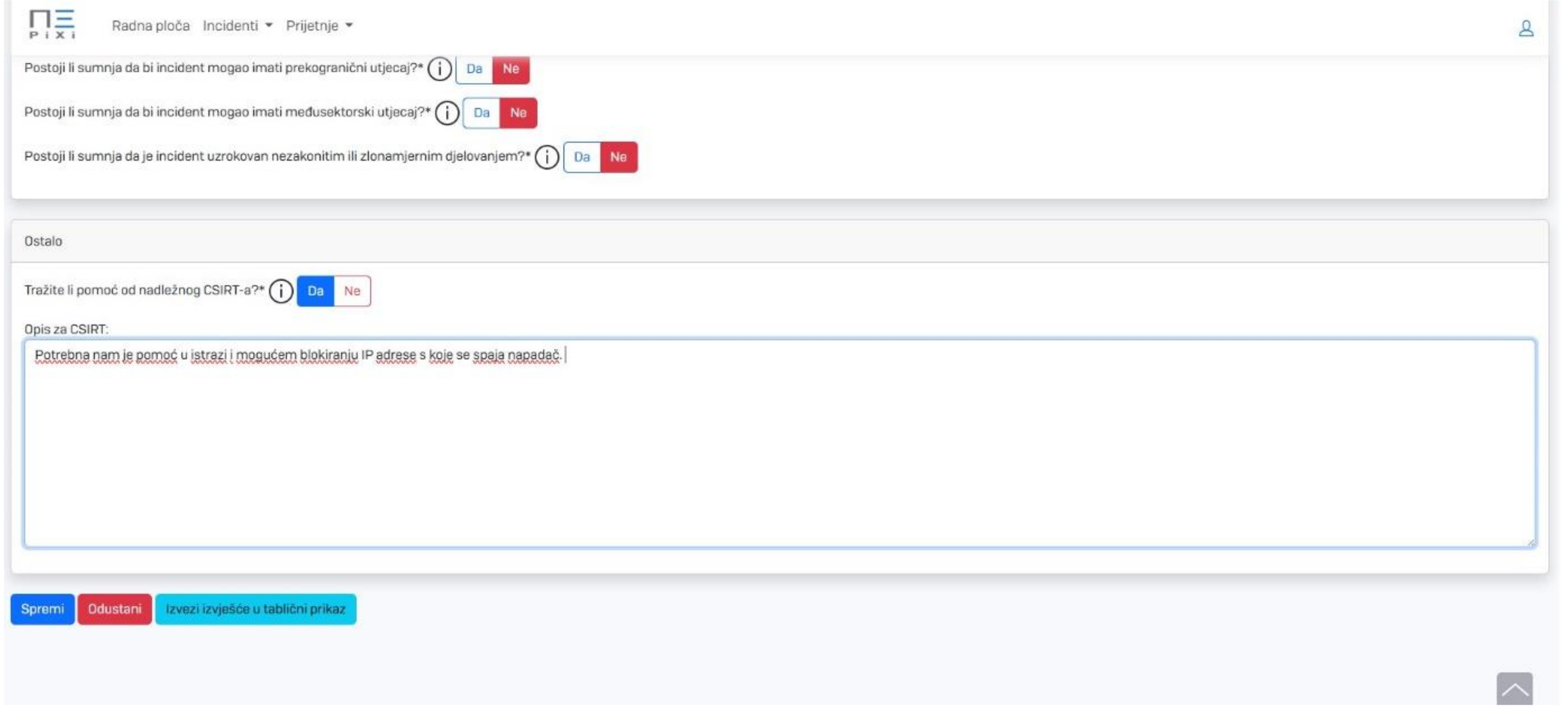
...

Opis incidenta*:

Kako je otkriven incident?
Koje je trenutno stanje incidenta?
Kronologija incidenta (timeline) koja je za sada otkrivena
Koji su poslovni procesi zahvaćeni incidentom i kakav je utjecaj na njih?
Ima li indikacije da su ukradeni (eksfiltrirani) podaci, i ako da koji?
Tko je sve uključen u rješavanje incidenta i u kojoj ulozi (djelatnici subjekta, vanjske firme koje npr. održavaju opremu, incident response firme)?
Koje su (za sada) planirane i poduzete mjere za odgovor na incident odnosno oporavak od incidenta?


PIXI
Radna ploča
Incidenti
Prijetnje
Indikatori kompromitacije:
Utvrđen je pristup mreži s IP adrese 193.198.252[.]44 u kojem je su uneseni korisnički podaci djelatnika. Adresa ne spada u IP raspon tvrtke.
Prilozi:
Dodaj ...
ulaz e-ovlaštenja.png (297.25 KB)


Radna ploča
Incidenti
Prijetnje
Utjecaji
Postoji li sumnja da se radi ili da bi moglo doći do napada putem opskrbnog lanca?*
Da
Ne
Dodatne informacije:
E-poruka je stigla s adrese / iz domene dugogodišnjeg dobavljača.
Postoji li sumnja da bi incident mogao imati prekogranični utjecaj?*
Da
Ne
Postoji li sumnja da bi incident mogao imati međusektorski utjecaj?*
Da
Ne
Postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem?*
Da
Ne


Radna ploča
Incidenti
Prijetnje
Postoji li sumnja da bi incident mogao imati prekogranični utjecaj?*
Da
Ne
Postoji li sumnja da bi incident mogao imati međusektorski utjecaj?*
Da
Ne
Postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem?*
Da
Ne
Ostalo
Tražite li pomoć od nadležnog CSIRT-a?*
Da
Ne
Opis za CSIRT:
Potrebna nam je pomoć u istrazi i mogućem blokiranju IP adrese s koje se spaja napadač.
Spremi
Odustani
Izvezi izvješće u tablični prikaz

Prateći dokumenti

- Taksonomija kibernetičkih incidenata
  - https://www.cert.hr/wp-content/uploads/2025/04/Nacionalna-taksonomija-kibernetickih-incidenata.pdf

- Opće smjernice za provedbu obveze obavještavanja o značajnim kibernetičkim incidentima
  - https://www.cert.hr/wp-content/uploads/2025/04/opce_smjernice_znacajni_incidenti.pdf

- Korisničke upute za korištenje Platforme PiXi

Izvještavanje prema Uredbi Dora

- Financijske institucije na koje se primjenjuje uredba DORA obvezne su obavijestiti svoja nadležna tijela/regulatore i CSIRT u slučaju značajnih incidenata koji utječu na kontinuitet pružanja usluga
- PiXi platforma se koristi za izvještavanje:
- Početna obavijest o incidentu sa znatnim učinkom
- Privremeno izvješće o incidentu sa značajnim utjecajem
- Završno izvješće o incidentu sa značajnim učinkom
- Za dobrovoljno izvješćivanje o kibernetičkim prijetnjama također će se koristiti PiXi platforma

PiXi u produkciji

- PiXi od 5. svibnja podržava proces prijave značajnih incidenata prema Zakonu o kibernetičkoj sigurnosti
  - kao i prijave na dobrovoljnoj bazi
- Funkcionalnosti koje podržavaju procese izvještavanja prema Uredbi Dora su u fazi testiranja

- Prijavljivanjem informacija o kibernetičkim incidentima i prijetnjama pomažemo povećati zajedničku otpornost na kibernetičke prijetnje

HVALA NA PAŽNJI!

ncert@cert.hr

incident@cert.hr

pixi.carnet.hr

CERT.hr