TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU

NKS NACIONALNO KOORDINACIJSKO SREDIŠTE

CARNET

Kibernetički incidenti i obveze prijave: uloga PiXi platforme

Jakov Kiš

Treća nacionalna NKS konferencija

26. svibnja 2026.

PiXi

Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima.

Razvoj i upravljanje Platformom PiXi u nadležnosti je CARNET-a.

Korištenje Platforme PiXi namijenjeno je isključivo ovlaštenim osobama (eOvlaštenja).

Pristup PiXi-u

Nadležna institucija uvela subjekt u PiXi

- ne treba čekati s prijavom u sustav do prvog incidenta

Davanje ovlaštenja kroz **eOvlaštenja**

- potreban **hrvatski OIB**
- ovlaštenje pristupa u PiXi može imati više osoba

Pristupa se putem pixi.carnet.hr autentifikacija putem NIAS-a

- značajna ili visoka razina vjerodajnice

Ovlaštena osoba ne treba imati posebna znanja iz područja kibernetičke sigurnosti, ali je poželjno da ima.

CEO vs NIAS admin vs PiXi korisnik

Može, a i ne mora biti ista osoba.

Strateška Vs. Operativna odgovornost.

Direktor mora i sam sebe ovlastiti ako želi pristup PiXi-u.

Obveza prijave incidenta

Subjekti su zakonski obvezni prijavljivati **značajne incidente.**

- svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 59. do 62. navedene Uredbe, uzimajući u obzir kriterijske pragove, kada su propisani.

Za subjekte iz članka 22. ZKS-a, primjenjuju se posebna pravila za utvrđivanje slučajeva u kojima se incident smatra značajnim prema Provedbenoj uredbi Komisije (EU) 2024/2690.

Vrste obavijesti i rokovi

Rano upozorenje – bez odgode, a najkasnije u roku od 24 sata od trenutka saznanja za značajan incident.

Početna obavijest – bez odgode, a najkasnije u roku od 72 sata od trenutka saznanja za značajan incident.

Privremeno izvješće – na zahtjev nadležnog CSIRT-a u zadanom roku (od 48 sati do 7 dana).

Završno izvješće – najkasnije u roku od 30 dana od dana dostave početne obavijesti o značajnom incidentu.

Izvješće o napretku – u slučaju da nije moguće dostaviti završno izvješće unutar roka jer incident još traje, dostavlja se izvješće o napretku umjesto završnog izvješća; unutar svakih sljedećih 30 dana trajanja incidenta dostavlja se novo izvješće o napretku, odnosno završno izvješće ako je incident završen.

Prijava incidenata je pokazatelj zrelosti, odgovornosti i otpornosti sustava.

CERT.hr

Prijava značajnog incidenta putem PiXi-a

pixi.carnet.hr

CERT.hr

e-Građani
Informacije i usluge

FILTRIRAJTE E-USLUGE | PRIJAVA | AA

Dobrodošli na PiXi!

PiXi

CERT.hr CARNET

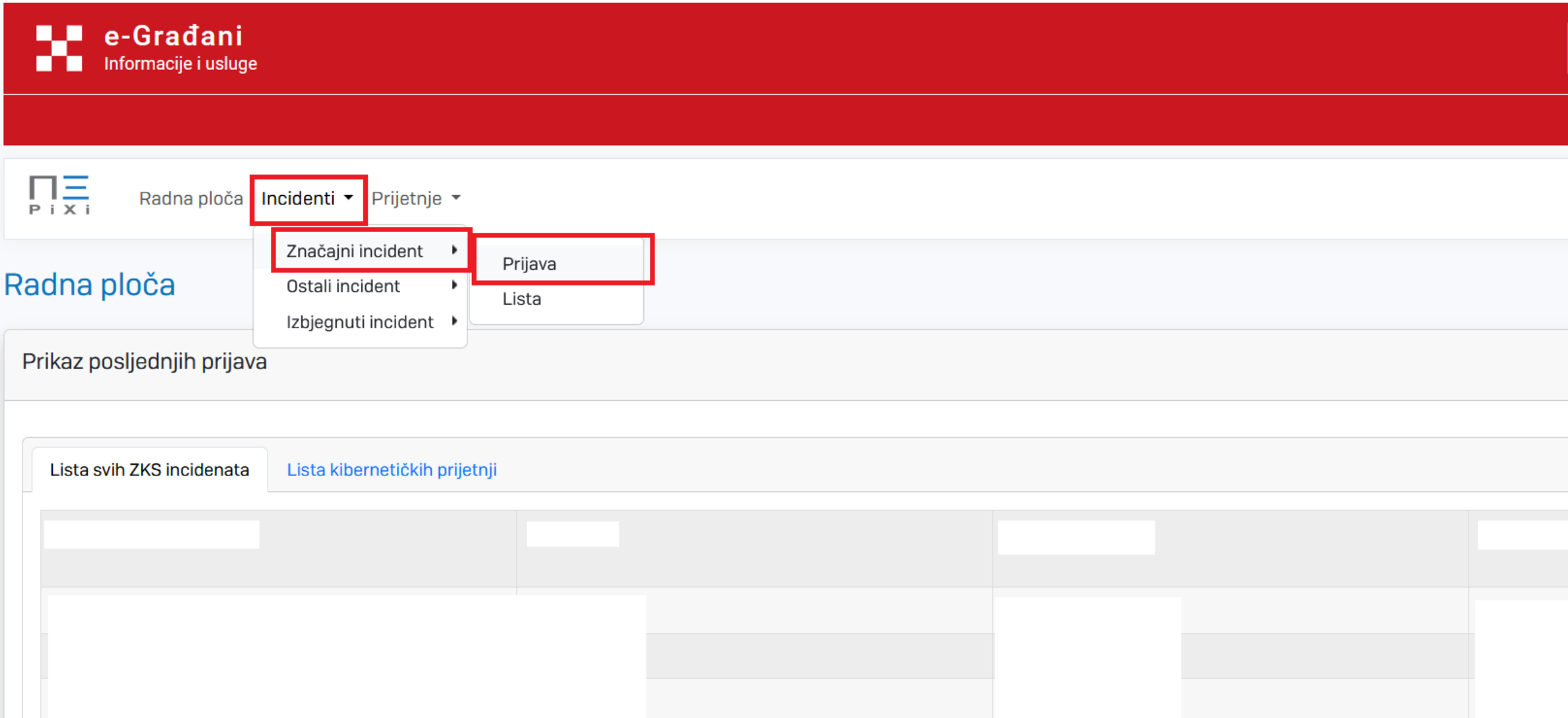
Platforma PiXi je **Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima** prema članku 43. Zakona o kibernetičkoj sigurnosti (NN 14/2024), Poglavlju IV. Uredbe o kibernetičkoj sigurnosti (NN 135/2024) i članku 15. Zakona o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor (NN 136/2024).

Razvoj i upravljanje Platformom PiXi u nadležnosti je CARNET-a.

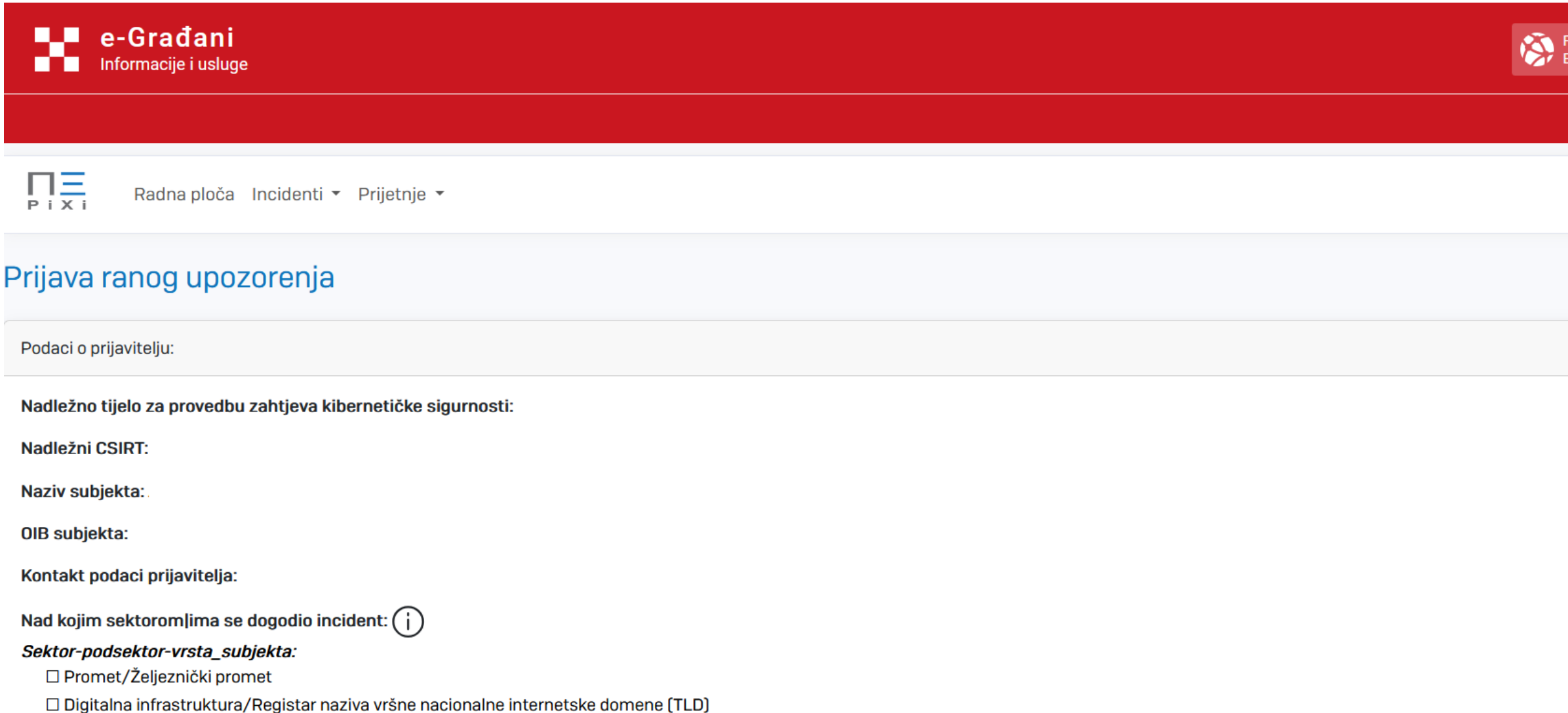
Korištenje Platforme PiXi namijenjeno je isključivo ovlaštenim osobama.

Odabir vjerodajnice

Odabir incidenta za prijavu



Rano upozorenje



Odabir kriterija

Kriteriji

Po kojim kriterijima je incident značajan:

Incidenti koji negativno utječu na dostupnost usluge ili narušavaju kvalitetu usluge

- ☐ najmanje 1 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje osam sati, pod uvjetom da 1 % primatelja usluge čini najmanje 100 primatelja uslu
- ☐ 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 vreme
- ☐ najmanje 30 % primatelja usluge povremeno nije moglo pristupiti usluzi ili nije moglo uslugu funkcionalno koristiti zbog smanjene razine kvalitete usluge, ako su po
- ☐ pristup usluzi u bolnici, zračnoj luci, zračnom prijevozniku, objektu banke s podatkovnim centrima, objektu policijskog sustava, aktivnom vodocrpilištu i centru upra
- ☐ pristup usluzi kontrole zračnog prometa nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna
- ☐ pristup usluzi koja se koristi za potrebe Ministarstva obrane i Oružanih snaga Republike Hrvatske, civilnih nositelja obrambenog planiranja, odnosno za potrebe prav
- ☐ najmanje 20 % primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje jedan sat
- ☐ pristup usluzi na području najmanje jedne županije ili jednog velikog grada ili grada koji predstavlja sjedište županije nije bio moguć u trajanju od najmanje jedan sat
- ☐ pristup usluzi Centra 112 i drugih hitnih službi nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna

Incidenti koji imaju ili mogu imati negativan učinak na autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga

- ☐ kritičnim dijelovima mrežnog i informacijskog sustava subjekta ili kritičnim podacima ostvaren je pristup od strane neovlaštene osobe ili su stečeni preduvjeti za os
- ☐ kritični mrežni i informacijski sustavi subjekta konfigurirani su od strane neovlaštene osobe ili su stečeni preduvjeti koji omogućavaju konfiguraciju kritičnog mrežn
- ☐ zbog incidenta su nastupile okolnosti koje onemogućuju ovlaštenoj osobi konfiguriranje kritičnog mrežnog i informacijskog sustava
- ☐ konfiguracija kritičnog mrežnog i informacijskog sustava subjekta neovlašteno je mijenjana, dopunjavana ili je iz drugih razloga postala nepouzdana ili su kritični po

Opći podaci o incidentu

Opći podaci

Kategorija incidenta:
Molimo odaberite potkategoriju - kategorija će se pokazati automatski!

Potkategorija incidenta*: ⓘ

Odaberi ...

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

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

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

Sažetak incidenta*: ⓘ

...

Opis osnovnih značajki 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?

Utjecaj

CERT.hr

Utjecaji

Postoji li sumnja na napad putem opskrbnog lanca* ⓘ Da Ne

Postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem*: ⓘ Da Ne

Procjena može li incident imati prekogranični utjecaj*: ⓘ Da Ne

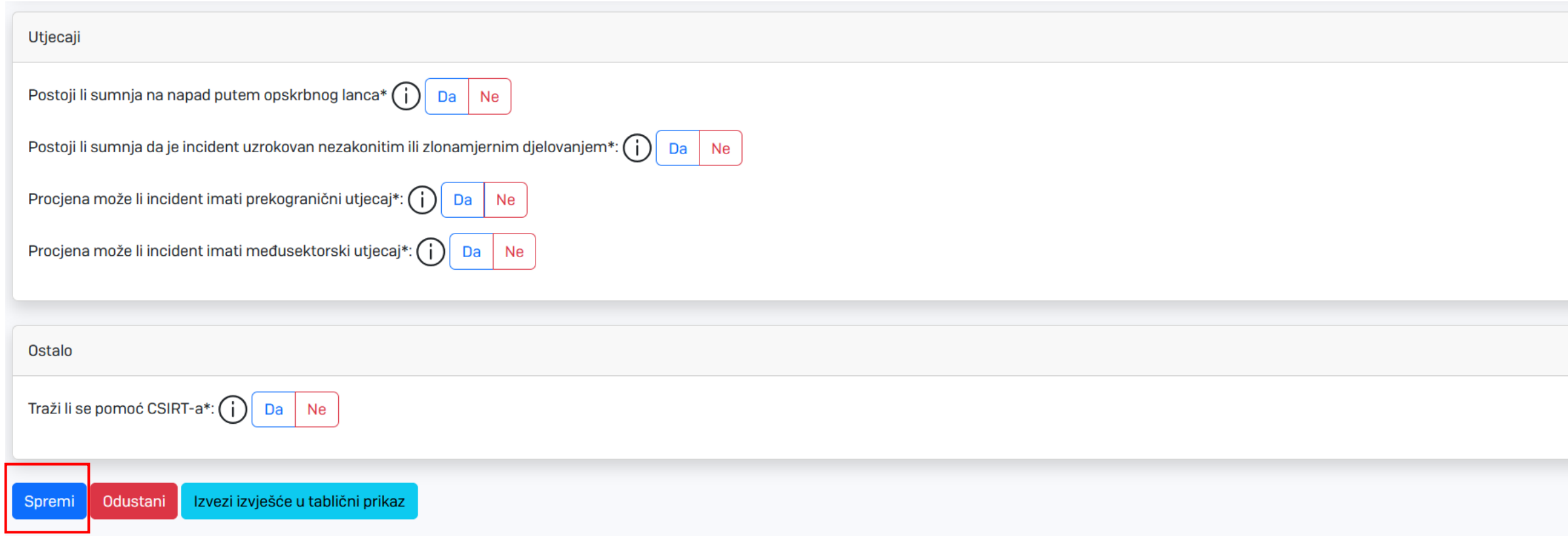
Procjena može li incident imati međusektorski utjecaj*: ⓘ Da Ne

Ostalo

Traži li se pomoć CSIRT-a*: ⓘ Da Ne

Spremi Odustani Izvezi izvješće u tablični prikaz

Spremi



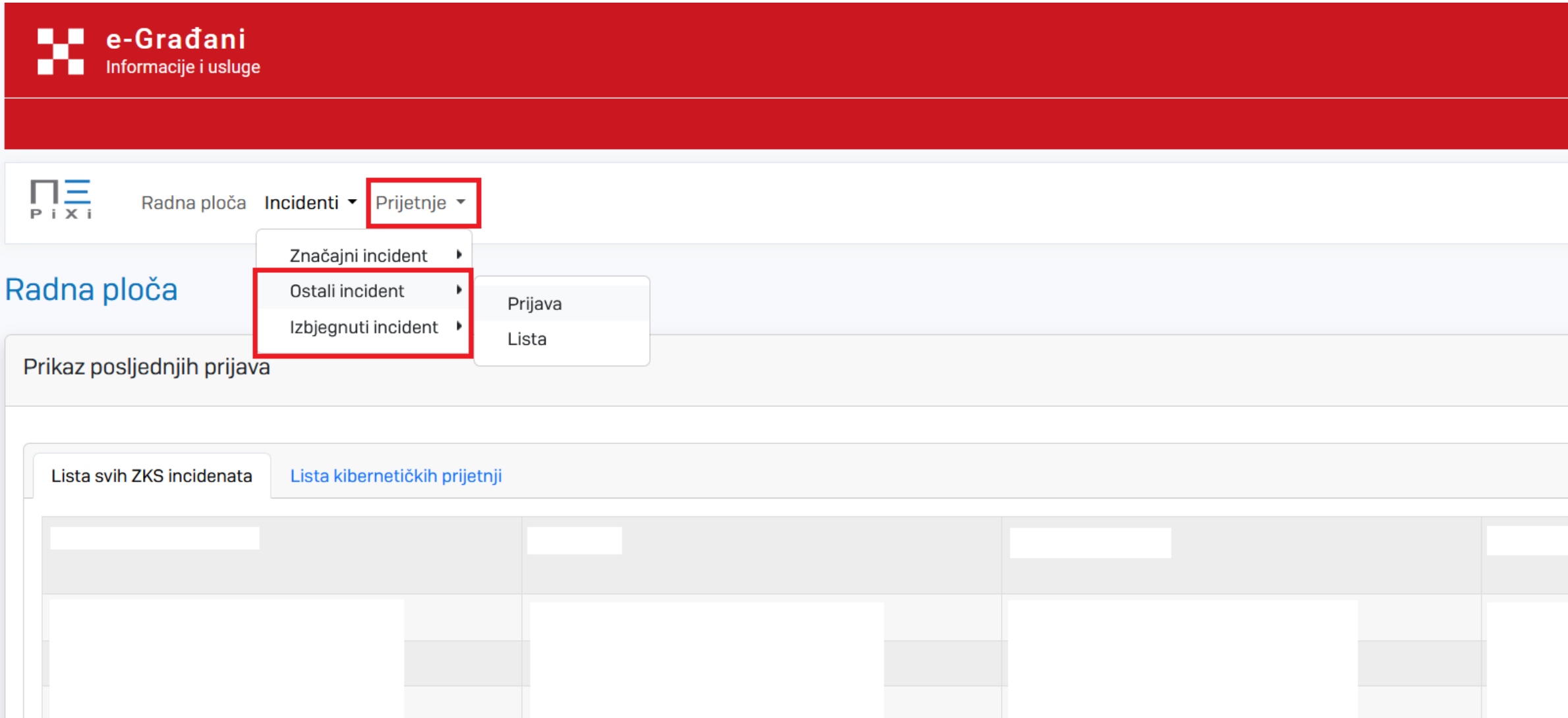
Nakon inicijalne prijave

Sustav podsjeća na druge obveze u propisanim rokovima.

Svi izvještaji se mogu predati jedan za drugim. Ne mora s čekati rok.

Popunjavanje izvještaja je moguće i nakon proteka roka za podnošenje, no **rokovi su zakonska obveza**!

Prijavite i druge incidente



Ako ne mogu pristupiti PiXi-u?*

Obrasce poslati na:

Nacionalni centar za kibernetičku sigurnost

incident@ncsc.hr

Nacionalni CERT

zks-incident@cert.hr

**subjekti trebaju naknadno unijeti informacije o značajnim incidentima na Platformu PiXi čim ona ponovno postane dostupna.*

Prijava je sigurna i povjerljiva

*Nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka dužna su, u skladu s pravom Europske unije i relevantnim nacionalnim pravom**, **čuvati sigurnost i komercijalne interese ključnih i važnih subjekata te povjerljivost dostavljenih informacija** u provedbi njihovih obveza sukladno ovoj Uredbi.*

Članak 6. Uredbe o kibernetičkoj sigurnosti

Prikrivanje incidenta najgori je mogući izbor.

- zakonski prekršaj
- ranjivosti ostaju otvorene
- povećavan rizik ponavljanja napada i ozbiljnijih posljedica.

Prednosti prijave incidenata

- Stručna pomoć i operativni savjeti
- Djelotvorno rješavanje ugroze
- Kolektivna zaštita i razmjena podataka

Prijavom incidenta subjekti prestaju biti prepušteni sami sebi u borbi protiv napadača te postaju dio koordiniranog nacionalnog sustava zaštite koji im pruža tehničku i analitičku potporu.

Hvala na pažnji.