Izgradnja spremnosti za NIS2 i jačanje sajber bezbjednosti i sajber otpornosti javnih institucija u Bosni i Hercegovini (interaktivno mapiranje nedostataka i planiranje implementacije za javnu upravu, okvir NIS2, odgovor na incidente, model CSIRT).

Organizovano u saradnji sa

Agencijom za državnu službu Bosne i Hercegovine i Zavoda za informatiku i statistiku Kantona Sarajevo

30/11- 2/12/2026

Mjesto: ***Naknadno će biti definisano***

Sarajevo, Bosna I Hercegovina

Korisnik:

Bosna i Hercegovina

TAIEX Case ID ETT 93837

Ciljevi radionice:

Radionica ima za cilj jačanje spremnosti za sajber bezbjednost, digitalnog upravljanja i institucionalnih kapaciteta javne uprave Bosne i Hercegovine, u skladu sa Direktivom NIS2 (Direktiva (EU) 2022/2555) i relevantnim dobrim praksama, standardima i pristupima EU u oblasti implementacije. Radionica je namijenjena državnim službenicima, IT stručnjacima, stručnjacima za sajber bezbjednost i pravnim stručnjacima odgovornim za upravljanje, rukovođenje i zaštitu IKT infrastrukture.

Radionica će ostvariti sljedeće međusobno povezane ciljeve:

- **Jačanje razumijevanja pravnog i regulatornog okvira** pružanjem učesnicima praktičnih znanja o Direktivi NIS2, uključujući njene zahtjeve u pogledu upravljanja rizicima, prijavljivanja incidenata, upravljanja, odgovornosti, nadzora i institucionalnih nadležnosti. Diskusije će doprinijeti boljem razumijevanju pravnih i regulatornih koraka potrebnih za dalje usklađivanje sa okvirom NIS2.
- **Unapređenje institucionalnog upravljanja i stručnih kapaciteta** kroz razmatranje uloga, odgovornosti, mehanizama koordinacije i struktura odgovornosti neophodnih za efikasno upravljanje sajber bezbjednošću u javnoj upravi. Posebna pažnja biće posvećena jačanju kompetencija IT stručnjaka i pravnih stručnjaka uključenih u upravljanje sajber bezbjednošću i usklađenost sa propisima.
- **Procjena trenutne spremnosti za sajber bezbjednost kroz interaktivno mapiranje nedostataka**, omogućavanjem učesnicima da sistematski analiziraju postojeće politike, procese, prakse upravljanja rizicima, procedure za prijavljivanje incidenata i tehničke okvire svojih institucija u odnosu na dobre prakse usklađene sa NIS2 okvirom.
- **Razvoj realistične mape puta** za implementaciju identifikovanjem prioritetnih pravnih, institucionalnih, tehničkih i strateških mjera, definisanjem praktičnih narednih koraka i uspostavljanjem strukturirane osnove za unapređenje sajber otpornosti javne uprave Bosne i Hercegovine. Kroz razmjenu iskustava sa ekspertima iz EU, učesnicima će biti pružena podrška u pretvaranju identifikovanih nedostataka u izvodljive korake implementacije i institucionalne prioritete.

Predavači:

- **Mr. Danut MAFTEI, PhD**
  Viši stručnjak za sajber bezbjednost
  Nacionalna direkcija za sajber bezbjednost *(eng. National Cyber Security Directorate – DNSC),* Rumunija
- **Mr Mihail George GURANDA**
  Bivši viši rukovodilac za sajber bezbjednost
  Nacionalna direkcija za sajber bezbjednost *(eng. National Cyber Security Directorate – DNSC),* Rumunija
- **Mr. Jan RADA**
  Viši pravni i politički savjetnik
  Nacionalna agencija za sajber i informacionu bezbjednost *(eng. National Cyber and Information Security Agency* -NÚKIB)
- **Mr Martin ŠVÉDA**
  Viši pravni savjetnik
  NÚKIB, Czech Republic
- **Mr Deividas STUMBRAS**
  Rukovodilac Odjeljenja za inovacije i tehnologiju
  Nacionalni centar za sajber bezbjednost *(eng. National Cyber Security Centre - NCSC)*, Litvanija
- **Mrs Eglė IVANOVAITĖ**
  Rukovoditeljica Odjeljenja za istrage incidenata
  Nacionalni centar za sajber bezbjednost *(eng. National Cyber Security Centre - NCSC)*, Litvanija

Data Protection: *Personal data contained in this document is processed in accordance with the privacy statement of the TAIEX instrument in compliance with Regulation (EU) 2018/1725. The chairperson should inform all persons attending the event that photographs/pictures should only be taken during a set period of time to allow for persons who do not agree to have their photographs taken to leave the room, unless all of the participants have provided their express consent to having their photograph taken.*

See

https://enlargement.ec.europa.eu/document/download/fc180dd7-6649-4914-875e-45fc4429ff83_en?filename=taiex_privacy_statement.pdf

Prvi dan: ponedeljak, 30. novembar 2026. godine	
Chair: Mr. Danut MAFTEI, PhD, Senior Cyber Security Expert, DNSC, Romania	
8:30 – 09:00	*Registracija učesnika, networking i tehničke provjere*
09:00 – 09:30	**Pozdravne riječi i uvod** - Stanje sajber bezbjednosti u Bosni i Hercegovini
09:30 – 10:15	**EU politike, strategije i pravni okvir u oblasti sajber pitanja** Sajber bezbjednost. Osnovni izazovi za građane, demokratske institucije i kritičnu informacionu infrastrukturu (kritične operatore); – EU pravni okvir u oblasti sajber bezbjednosti. – Nacionalne politike i strategije sajber bezbjednosti koje oblikuju razvoj nacionalnog pravnog okvira u oblasti sajber pitanja. **Govornik**: Mr. Danut MAFTEI, PhD, Viši stručnjak za sajber bezbjednost, DNSC, Romania
10:15 – 11:00	**Kako procijeniti spremnost javne uprave za NIS2: od zahtjeva do institucionalnih nedostataka** – Prevođenje zahtjeva NIS2 u praktična pitanja za institucije; – Identifikovanje uloga, kritičnih usluga, IKT zavisnosti i postojećih mjera sajber bezbjednosti; – Mapiranje politika, procesa, odgovornosti i dokaza u odnosu na zahtjeve usklađene sa NIS2; – Izrada praktične matrice nedostataka i identifikovanje prioritetnih oblasti za unapređenje. **Govornik:** Mr Jan RADA, Viši pravni i politički savjetnik, Nacionalna agencija za sajber i informacionu bezbjednost *(eng. National Cyber and Information Security Agency* - NÚKIB), Češka Republika
11:00 – 11:30	*Pauza*
11:30 – 12:15	**Od NIS2 do Zakona o sajber bezbjednosti u Litvaniji: praktična implementacija i naučene lekcije** – Model upravljanja sajber bezbjednošću; – Područje primjene i obuhvaćeni subjekti; – Uspostava saradnje (“Onboarding”) – Naučene lekcije: šta je funkcionisalo, gdje su se institucije suočavale sa poteškoćama i šta bismo uradili drugačije (predstojeće promjene). **Govornik:** Mr Deividas STUMBRAS, rukovodilac Odjeljenja za inovacije i tehnologiju, Nacionalni centar za sajber bezbjednost (*eng. National Cyber Security Centre-NCSC*), Litvanija

12:15 – 13:00	**Od NIS2 do Zakona o sajber bezbjednosti u Češkoj Republici: praktična implementacija i naučene lekcije** – Model upravljanja sajber bezbjednošću – Područje primjene i obuhvaćeni subjekti – Uspostava saradnje ("Onboarding") – Naučene lekcije: šta je funkcionisalo, gdje su se institucije suočavale sa poteškoćama i šta bismo uradili drugačije (predstojeće promjene). **Speaker:** Mr Martin SVEDA, Viši pravni stručnjak, Nacionalna agencija za sajber i informacionu bezbjednost *(eng. National Cyber and Information Security Agency* - NÚKIB), Češka Republika
13:00 – 14:00	*Pauza za ručak* *Molimo vas da ne zaboravite potpisati listu prisustva*
14:00 – 14:45	**Mjere bezbjednosti (član 20. i 21. NIS2 Direktive) – Različita stanovišta** – Obaveze utvrđene članom 20. i 21. NIS2 Direktive – Provedbena uredba Komisije (EU) 2024/2690 – Nacionalna transpozicija u Češkoj Republici. **Govornik**: Mr Martin SVEDA
14:45 – 15:30	**Centri za bezbjednosne operacije (SOC)** – Nacionalni ekosistem i zakonodavna osnova za SOC centre u Republici Litvaniji; – Projektovanje SOC centara; – Procjena zrelosti i pružene usluge. **Govornik:** Ms Egle IVANOVAITE, Rukovoditeljica Odjeljenja za istrage incidenata, NCSC, Litvanija
15:30 – 16:00	*Pauza*
16:00 – 16:45	**Unapređenje nacionalne sajber otpornosti. Nacionalna direkcija za sajber bezbjednost Rumunije (DNSC)** – Pravni okvir za uspostavljanje DNSC-a; – Upravljanje i osoblje; – Ciljevi, funkcije i odgovornosti; – Saradnja i razmjena informacija. **Govornik:** Mr. Danut MAFTEI
16:45 – 17:00	Ostala pitanja Pitanja i odgovori Zaključak prvog dana

Drugi dan: utorak, 01. decembar 2026. godine	
Predsjedavajući: Mr. Danut MAFTEI, PhD, Viši stručnjak za sajber bezbjednost, DNSC, Romania	
08:30 – 09:00	*Registracija učesnika, networking i tehničke provjere*
09:00 – 09:45	**Koordinisano objavljivanje informacija o ranjivostima i upravljanje ranjivostima u okviru NIS2 Direktive** – CVD i upravljanje ranjivostima u okviru NIS2; – Uloge nadležnih organa, CSIRT-ova, organizacija i istraživača bezbjednosti; – Od prijavljivanja ranjivosti do koordinacije, otklanjanja i objavljivanja informacija; – Praktične lekcije iz češkog pristupa koordinisanom objavljivanju informacija o ranjivostima. **Govornik:** Mr Jan RADA
09:45 – 10:30	**Uspostavljanje CERT-a: od pravnog mandata do operativnih kapaciteta** – Pravne i institucionalne osnove za uspostavljanje CERT-a (mandat, pozicioniranje u okviru vlasti, model upravljanja); – Osnovne funkcije CERT-a i mapa puta zrelosti: postupanje u slučaju incidenata, koordinacija, rano upozoravanje; – Kadrovski kapaciteti, resursi i međuinstitucionalna saradnja. Dobre prakse DNSC-a Rumunije. **Govornik:** Mr. Mihail George GURANDA, Bivši viši rukovodilac za sajber bezbjednost, Nacionalna direkcija za sajber bezbjednost *(eng. National Cyber Security Directorate – DNSC)*, Rumunija
10:30 – 11:15	**Od strategije do implementacije: kako razviti efikasnu nacionalnu strategiju sajber bezbjednosti (primjer Češke Republike)** – Od procjene i strateških ciljeva do konkretnih mjera i prioriteta; – Mapiranje zainteresovanih strana, institucionalne odgovornosti i koordinacija na nivou cijele vlasti; – Izrada planova implementacije: odgovornost za realizaciju, ključne etape, resursi i mjerljivi rezultati; – Naučene lekcije iz razvoja i implementacije strategija sajber bezbjednosti u Češkoj Republici. **Govornik:** Mr Jan RADA
11:15 – 11:45	*Pauza*

11:45 – 12:30	**Nacionalni odgovor na incidente i kontinuitet** – Institucionalno otkrivanje i odgovor na incidente – uloge, odgovornosti i koordinacija; – Prijavljivanje incidenata, komunikacija i pravni aspekti – zahtjevi za prijavljivanje, očuvanje dokaza, komunikacija i donošenje odluka; – Interaktivna diskusija o upravljanju incidentima u institucijama – identifikovanje izazova i dobrih praksi u koordinaciji tehničkog i pravnog odgovora. **Govornik:** Ms Egle IVANOVAITE
12:30 – 13:15	**Razmjena informacija i situaciona svijest** – Integracija podataka o prijetnjama; – Sistemi ranog upozoravanja; – Nacionalno izvještavanje o situaciji; – Nacionalni DNS Firewall. Zakonodavstvo, tehnička implementacija i rezultati. **Govornik:** Mr Deividas STUMBRAS
13:15 – 14:15	*Pauza za ručak* *Molimo vas da ne zaboravite potpisati listu prisustva.*
14:15 – 15:00	**Rizici, prijetnje i ranjivosti povezane sa proizvodima i komponentama sa digitalnim elementima. Laboratorije za testiranje** – Rizici, prijetnje i ranjivosti povezane sa proizvodima i komponentama sa digitalnim elementima koje koriste vladin sektor i kritična informaciona infrastruktura (CIIP); – Ranjivosti u oblasti bezbjednosti identifikovane u LTE i 5G tehnologiji koje predstavljaju rizik za građane, poslovne subjekte, državne institucije, CIIP i nacionalnu bezbjednost; – Laboratorije za testiranje IKT proizvoda, IKT usluga i IKT procesa. **Govornik**: Mr. Danut MAFTEI
15:00 – 15:45	**Od obaveza izvještavanja prema NIS2 do operativnih procedura za postupanje u slučaju incidenata** – **Rokovi za prijavljivanje;** – **Klasifikacija incidenata i nivoi ozbiljnosti;** – **Interna matrica eskalacije;** – **Šta institucija mora imati uspostavljeno prije početka računanja roka.** **Govornik:** Mr Deividas STUMBRAS
15:45 – 16:30	Ostala pitanja Pitanja i odgovori Zaključak prvog dana

Treći dan: srijeda, 02. decembar 2026. godine	
Predsjedavajući: Mr. Danut MAFTEI, PhD, Viši stručnjak za sajber bezbjednost, DNSC, Romania	
08:30 – 09:00	*Registracija učesnika, networking i tehničke provjere*
09:00 – 09:45	**Izrada standardnih operativnih procedura za operacije sajber bezbjednosti** – **Pregled standarda;** – **Teme procedura;** – **Implementacija procedura;** – **Preispitivanje i izgradnja zrelosti.** **Govornik:** Ms Egle IVANOVAITE
09:45 – 10:30	**CERT aktivnosti i koordinacija incidenata u praksi** – Od otkrivanja do odgovora: operativni tokovi rada i koordinacija sa sektorskim CSIRT-ovima i nadležnim organima; – Razmjena informacija, situaciona svijest i mehanizmi ranog upozoravanja, – Praktične lekcije iz proširivanja aktivnosti CERT-a kroz kritične sektore u Rumuniji **Govornik:** Mr. Mihail George GURANDA
10:30 – 11:15	**Nacionalne strategije sajber bezbjednosti i javno-privatna partnerstva (PPP) u sajber bezbjednosti EU** – Karakteristike i pokretači za uspostavljanje javno-privatnih partnerstava; – Značaj javno-privatnih partnerstava u zaštiti kritične informacione infrastrukture. Klasifikacija i opis javno-privatnih partnerstava; – Modeli EU za javno-privatnu saradnju; prednosti i nedostaci javno-privatnih partnerstava; – Izazovi, izgradnja povjerenja i razmjena informacija. **Govornik**: Mr. Danut MAFTEI
11:15 – 11:45	*Pauza*
11:45 – 12:30	**Od operativne sajber bezbjednosti do strateškog upravljanja: pogled CISO-a na institucionalnu otpornost** – Povezivanje tehničkih kapaciteta CERT-a sa izvršnim nivoom upravljanja - uloga CISO-a u institucionalnoj sajber otpornosti; – Integrisanje usluga CERT-a u okvir upravljanja rizicima i usklađenosti institucije sa NIS2 direktivom; – Pretvaranje procjene nedostataka u institucionalni plan aktivnosti sa jasno definisanim prioritetima i potrebnim resursima. **Govornik:** Mr. Mihail George GURANDA
12:30 – 13:15	**Češki sistem sajber protivmjera – sajber otpornost izvan Direktive NIS2** – Uvod u češki sistem protivmjera; – Upozoravajuće i reaktivne protivmjere; – Praktični primjeri primjene protivmjere. **Govornik:** Mr Martin SVEDA
13:15 – 14:15	*Pauza za ručak* *Molimo vas da ne zaboravite potpisati listu prisustva.*

14:15 – 15:00	**Stanje sajber vanredne situacije – sajber otpornost izvan Direktive NIS2** – Uključivanje stanja sajber vanredne situacije u sistem upravljanja krizama u Češkoj Republici; – Pregled češkog stanja sajber vanredne situacije; – Mjere u slučaju stanja sajber vanredne situacije. **Govornik:** Mr Martin SVEDA
15:00 – 15:30	*Pauza*
15:30 – 16:15	**Završne diskusije** – Izazovi sajber bezbjednosti za BiH; – Diskusije u vezi sa očekivanim rezultatima događaja: – Diskusija radi definisanja oblasti za dalju saradnju sa Evropskom komisijom i ekspertima iz država članica EU; – Naredni koraci i nacionalna mapa puta; – Sesija pitanja i odgovora. **Govornik:** svi eksperti iz EU i učesnici
16:15 – 16:30	Pitanja i završne napomene / Kraj radionice



TAIEX 30

BETTER INSTITUTIONS, BETTER LIVES

ec.europa.eu/taiex

TAIEX@30: BETTER INSTITUTIONS, BETTER LIVES

ENEST-TAIEX@ec.europa.eu