TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU

NKS NACIONALNO KOORDINACIJSKO SREDIŠTE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HIKS HRVATSKI INSTITUT ZA KIBERNETIČKU SIGURNOST

HUP Hrvatska udruga poslodavaca

HGK HRVATSKA GOSPODARSKA KOMORA

CARNET

Program Digitalna Europa - što dolazi?

Karlo Vugrinec
Služba za poslove pružanja financijske potpore u području kibernetičke sigurnosti, PM za NCC-HR projekt

Što je Program Digitalna Europa?

- **Strateški instrument financiranja:**

Fokusiran na uvođenje digitalnih tehnologija u MSP, javnu upravu

- **Jačanje kritičnih kapaciteta:**

Prioritetna područja uključuju umjetnu inteligenciju (AI), kibernetičku sigurnost, superračunalstvo (HPC)

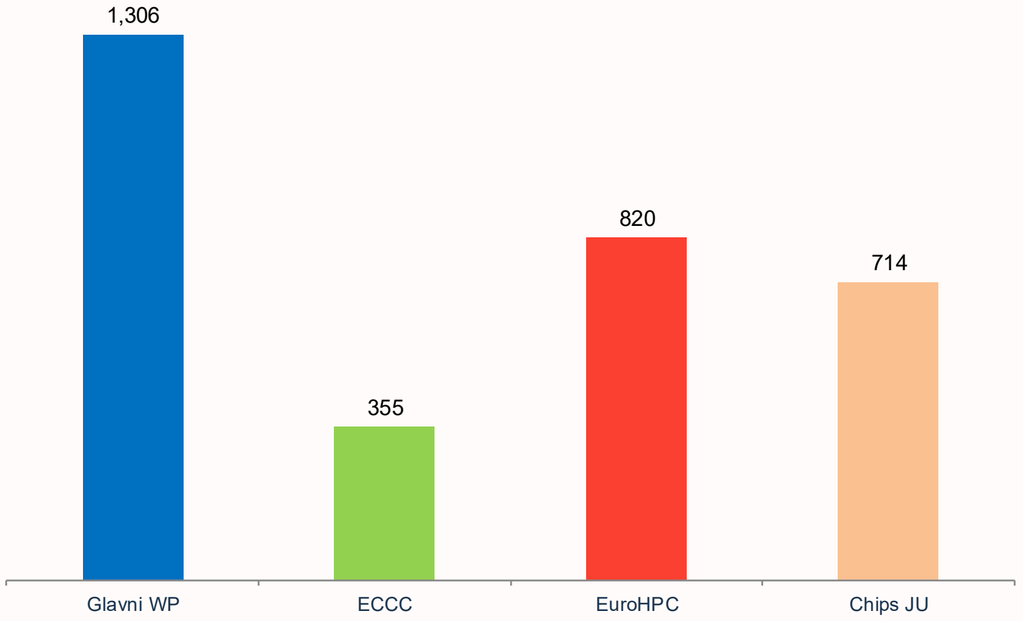
- **Tehnološka suverenost i sigurnost:**

Osigurava neovisnost Europe u ključnim visokotehnološkim lancima opskrbe i otpornost na kibernetičke prijetnje.

- **Razvoj naprednih vještina:**

Cilj je povećanje broja ICT stručnjaka kroz specijalizirane akademije (EDIH) za AI, kvantne tehnologije i virtualne svjetove.

Ukupan DEP proračun 2025–2027



Područje 3 - kibernetička sigurnost i povjerenje za razdoblje 2025-2027

- **139 milijuna EUR** za nove tehnologije i kibernetičku sigurnost, uvođenje umjetne inteligencije i kibernetičke sigurnosti te postkvantnu tranziciju.

- • **97 milijuna EUR** za provedbu Akta o kibernetičkoj solidarnosti, konsolidaciju Europskog sustava upozoravanja na kibernetičku sigurnost, Mehanizam za kibernetičke hitne situacije / aktivnosti pripravnosti, uzajamnu pomoć i uspostavu regionalnih kabelskih čvorišta.

- • **110 milijuna EUR** za dodatne mjere kojima se poboljšava kibernetička otpornost EU-a.

- • **9 milijuna EUR** za aktivnosti potpore programu

Areas and topics with indicative allocations (in million EUR)		2025	2026	2027	Total
New technologies, AI & post-quantum transition					**139**
2.1	Cybersecure tools, technologies and services relying on AI	15	15	15	45
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions		20		20
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	25			25
2.4	Transition to post-quantum Public Key Infrastructures	15			15
2.5	Migration of Cyber Hubs to PQC			4	4
2.6	Uptake of innovative cybersecurity solutions for SMEs	15		15	30
Cyber Solidarity Act and EU Action Plan on Cable Security Implementation					**97**
2.7	National Cyber Hubs	5	5		10
2.8	Cross-Border Cyber Hubs	5		15	20
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	10	15	15	40
2.11	Mutual assistance		2	2	4
2.12	Regional Cable Hubs	10	5	6	21
Additional actions improving EU cyber resilience					**110**
2.13	Enhancing the NCC Network	10	11	17	38
2.14	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	12	32
2.15	Dedicated action to reinforce hospitals and healthcare providers	30			30
2.16	Dual-use technologies		10		10
Programme Support Actions		3	3	3	9
TOTAL (in million EUR)		**143**	**108**	**104**	**355**

Cybersecure tools, technologies and services relying on AI

Očekivani ishodi

- Uvođenje AI tehnologija kao potpore kibernetičkim čvorištima, CSIRT-ovima, NCSC-ovima i drugim ključnim dionicima.
- Razvoj, testiranje i primjena novih AI alata za otkrivanje, analizu i obradu kibernetičkih prijetnji.
- Jačanje razmjene informacija i suradnje kroz AI-generirane obavještajne podatke o prijetnjama.
- Automatizacija procesa kibernetičke sigurnosti i unaprjeđenje operativnih kapaciteta Cyber Hubova.
- Razvoj sigurnih, pouzdanih i zakonodavno usklađenih AI rješenja za NIS sektore.
- Doprinos europskoj standardizaciji i certificiranju sigurnih AI tehnologija.

Cybersecure tools, technologies and services relying on AI

Prihvatljivi prijavitelji

- Pružatelji tehnoloških rješenja,
- Cyber-Hubs,
- istraživačka i akademska zajednica,
- subjekti za kibernetičku sigurnost,
- javni sektor,
- subjekti obuhvaćeni Direktivom NIS 2-ZKS, privatni sektor te drugi relevantni dionici koji podupiru uvođenje kibernetički sigurnih AI rješenja.

Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions

Očekivani ishodi

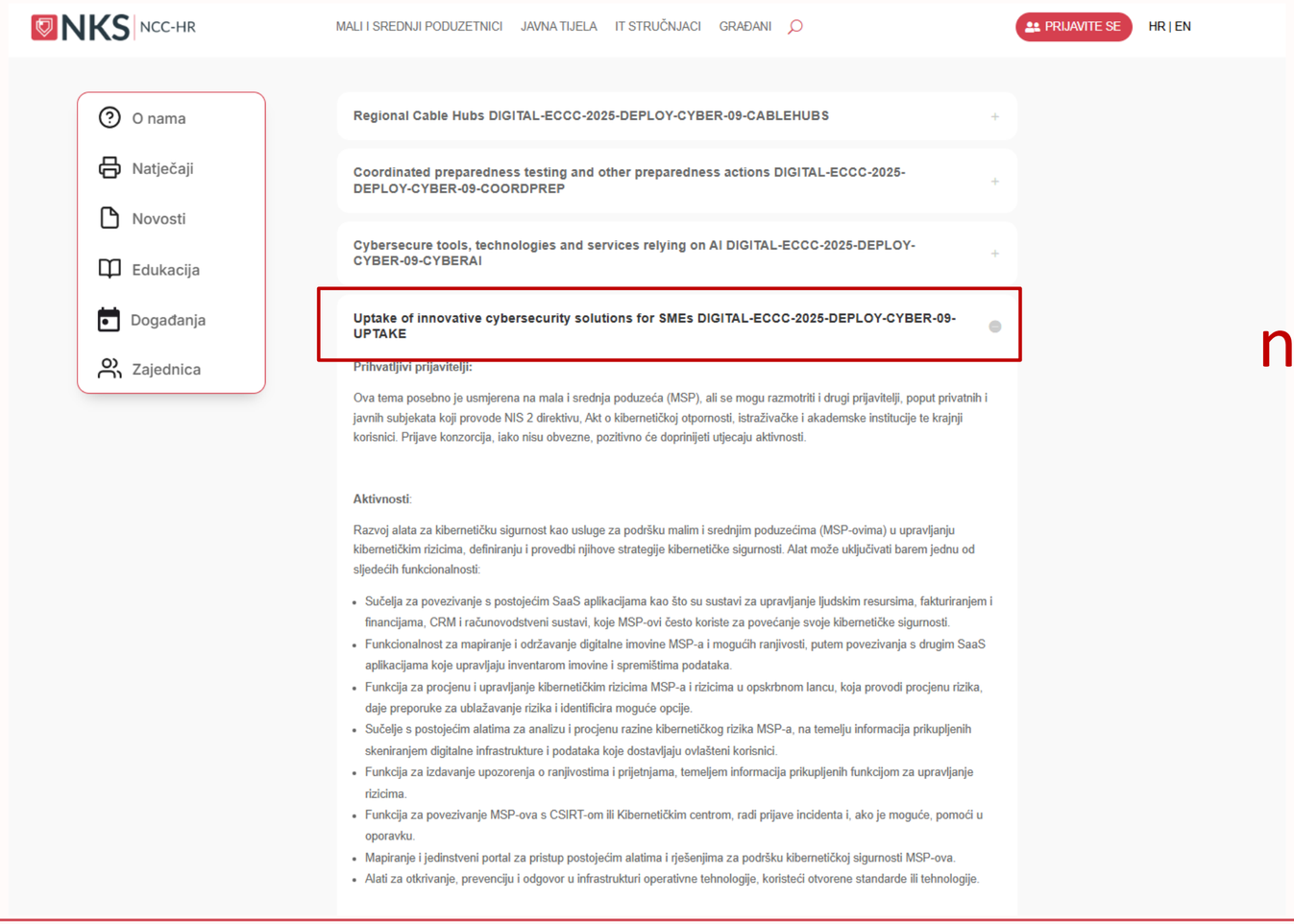
- Uvođenje tržišno spremnih inovativnih AI rješenja za kibernetičku sigurnost.Dostupnost ažurnih AI alata i usluga organizacijama, posebno MSP-ovima.
- Integracija AI tehnologija u procese kibernetičke sigurnosti radi jačanja sigurnosti IKT rješenja.Osposobljavanje zaposlenika za primjenu AI rješenja u kibernetičkoj sigurnosti.
- Primjena pouzdane umjetne inteligencije, AI alata za kibernetičku sigurnost i alata za zaštitu samih AI rješenja.

Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions

Prihvatljivi prijavitelji

- MSP-ovi,
- start-upovi,
- istraživačka i akademska zajednica,
- javni sektor,
- subjekti obuhvaćeni Direktivom NIS 2 te drugi industrijski akteri i relevantni dionici (uključujući dobavljače AI-powered rješenja)

Uptake of innovative cybersecurity solutions for SMEs -2027



nks.hr/natjecaji

Coordinated preparedness testing and other preparedness actions

Očekivani ishodi

Prvi dio

- Jačanje suradnje, pripravnosti i kibernetičke otpornosti u EU-u; usluge potpore pripravnosti.
- Usluge procjene prijetnji i procjene rizika.

Drugi dio

- Usluge praćenja rizika.
- Bolju usklađenost, koordinirano otkrivanje ranjivosti i praćenje.
- Unaprjeđenje vještina kroz vježbe i programe osposobljavanja, organizaciju događanja, radionica, savjetovanja s dionicima i izradu white-paper-a

Coordinated preparedness testing and other preparedness actions

Prihvatljivi prijavitelji

- Javna tijela u ulozi nadležnih tijela za kibernetičku sigurnost ili CSIRT-ova.
- Javna tijela obuhvaćena Direktivom NIS 2 i drugim relevantnim regulatornim okvirima, uključujući CRA, CSA, CSoA i DORA.

Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

Očekivani ishodi

- Provedba smjernica, standardiziranih procesa i priručnika za primjenu zakonodavstva o kibernetičkoj sigurnosti.
- Potpora MSP-ovima i industriji u usklađivanju s CRA zahtjevima, uključujući ocjenjivanje sukladnosti i certifikaciju.
- Smanjenje administrativnog opterećenja kroz alate poput jedinstvene točke/rješenja za prijavu incidenata.
- Uspostava sigurnih komunikacijskih kanala i jačanje razmjene informacija među dionicima.
- Razvoj treninga, vježbi, radionica i programa razmjene za jačanje kibernetičkih kapaciteta.
- Potpora obrazovanju, natjecanjima i razvoju budućih stručnjaka za kibernetičku sigurnost.
- Pilot-projekti, metodologije i dobre prakse za testiranje i dokazivanje CRA usklađenosti.
- Razvoj i primjena tehnologija koje jačaju sigurnost i privatnost u IKT proizvodima i uslugama.
- Jačanje suradnje između industrije, istraživača, korisnika, regulatora i tijela za zaštitu podataka.

Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

Prihvatljivi prijavitelji

- Svi dionici

Dual-use technologies

Očekivani ishodi

- Razvoj sigurnog i šifriranog okvira za razmjenu podataka između civilnih i vojnih dionika.
- Uspostava europskog sustava ranog upozoravanja na kibernetičke i hibridne prijetnje.
- Korištenje praćenja u stvarnom vremenu i prediktivne analitike za zaštitu kritične infrastrukture.
- Zajednički programi osposobljavanja za civilni, sigurnosni i vojni sektor.
- Uvođenje integriranih sustava za otkrivanje prijetnji temeljenih na AI-u, ZTA-u i digitalnim blizancima.
- Razvoj međusektorskih sigurnosnih standarda za tehnologije dvojne namjene.
- Jačanje suradnje nacionalnih tijela, MSP-ova, akademske zajednice i industrije.

Prihvatljivi prijavitelji

- Svi dionici

KAKO DO NAS?

@ mrežno sjedište

https://nks.hr/

@ LinkedIn

NCC-HR: Croatian Cybersecurity Coordination Centre

@ e-pošta

info@nks.hr

Hvala na pažnji.