

NKS: Prilike za podršku ulaganjima u kibernetičku sigurnost

Prezentira **Vlatka Marčan**, pomoćnica ravnatelja i voditeljica NKS-a



Analiza potreba u području kibernetičke sigurnosti



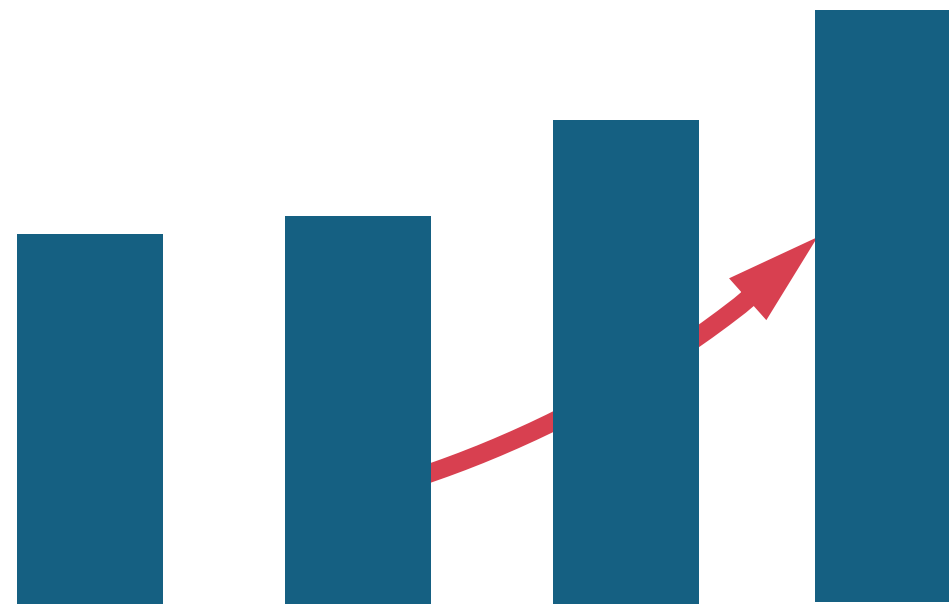


| Analiza potreba u području kibernetičke sigurnosti

- **Upitnik** (112 ispitanika) proveden u suradnji s HUP i HGK (srpanj – studeni 2024.)
- **Meet up u Osijeku** proveden u suradnji s NCSC-HR, CERT-om, Osijek Software Cityem, Osječko-baranjskom županijom (veljača 2025.)
- **Meet up u Splitu** proveden u suradnji s NCSC, CERT-om i Centrom izvrsnosti Splitsko-dalmatinske županije (ožujak 2025.)

I Upitnik: Veličina poduzeća

- **Velika poduzeća** (+250 zaposlenih):
33 odgovora
- **Srednja poduzeća** (50 – 249 zaposlenih):
31 odgovor
- **Mala poduzeća** (10 – 50 zaposlenih):
23 odgovora
- **Mikro poduzeća** (do 10 zaposlenih):
25 odgovora



I Upitnik: Stanje kibernetičke sigurnosti

IZLOŽENOST NAPADIMA

Većina organizacija (59%) smatra da nije bila izložena kibernetičkim napadima u prošlosti. Međutim, 32% ispitanika vjerojatnost budućeg napada ocjenjuje ocjenom 3 (na skali 1-6), dok 12% smatra da će sigurno biti pogođeni u idućoj godini.

SUSTAVI ZAŠTITE

51% organizacija ima razvijen sustav kibernetičke sigurnosti, dok 54% koristi samo bazične alate i rješenja. Napredne alate koristi tek 33% organizacija, a 13% ne koristi nikakve alate za kibernetičku sigurnost.

KADROVI

Čak 29% organizacija nema zaposlenika koji se bavi kibernetičkom sigurnošću, dok samo 15% ima organizacijsku jedinicu koja se bavi isključivo tim pitanjima. Velika poduzeća imaju najviše zaposlenih u IT organizacijskim jedinicama.



I Upitnik: Edukacije u području kibernetičke sigurnosti

63%

PLAN EDUKACIJE

Organizacija koje imaju sustavni plan edukacije zaposlenika. Velika poduzeća u najvećem broju imaju plan edukacija za teme vezane uz kibernetičku sigurnost



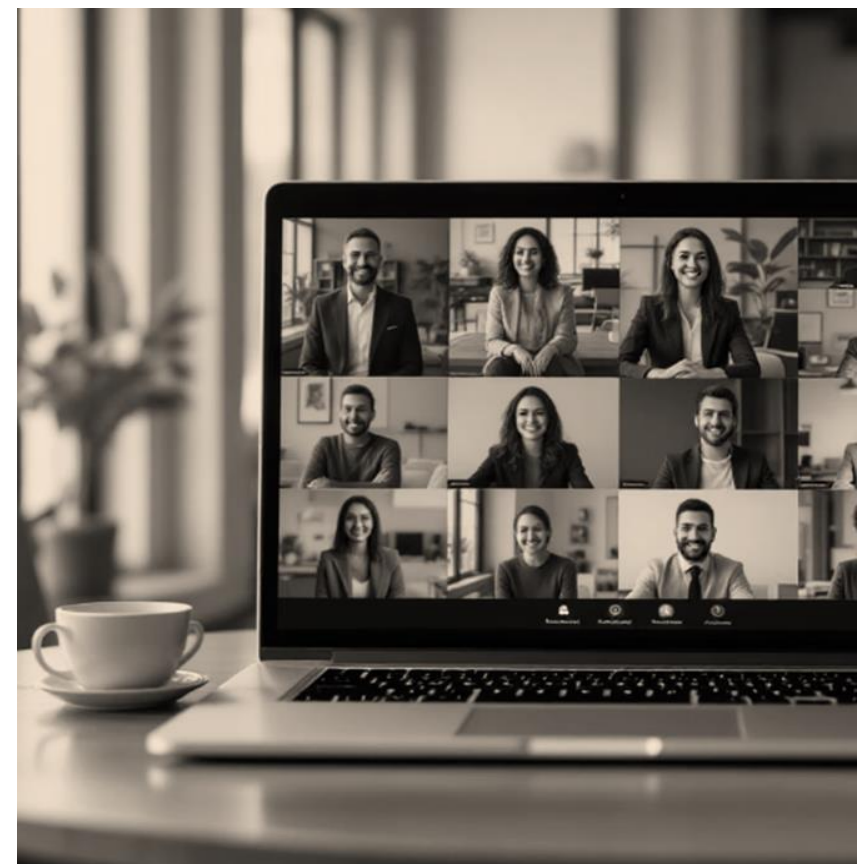
I Upitnik: Sudjelovanje i preferirani oblici edukacija

TKO TREBA SUDJELOVATI NA EDUKACIJAMA?

- 47% menadžment
- 47% voditelji organizacijskih jedinica
- 45% djelatnici za kibernetičku zaštitu

NAJPOPULARNIJI OBLIK EDUKACIJA

- 42% preferira kratke online edukacije
- 13% preferira višednevne edukacije uživo



I **Upitnik:** Financijski planovi za kibernetičku sigurnost u poduzećima

Prema istraživanju, 56 % ispitanika u svojim godišnjim financijskim planovima predviđa sredstva za nabavu novih sigurnosnih rješenja, edukacija ili praksi iz područja kibernetičke sigurnosti.



I Upitnik: Pregled raspodjele sredstava i strategija po veličini poduzeća

PROCJENA TROŠKOVA ZA RAZVOJ ILI NABAVU SIGURNOSNIH RJEŠENJA

55% ispitanika očekuje troškove do 20.000 €

15% ispitanika očekuje troškove od 20.000 do 40.000,00 €

9% ispitanika očekuje troškove od 40.000 do 60.000 €

22% očekuje troškove veće od 60.000 €





I Meet up: Stanje educiranosti o kibernetičkoj sigurnosti

KIBERNETIČKA SIGURNOST

Svijest o važnosti kibernetičke sigurnosti raste, no još postoji značajan jaz u razini praktične edukacije među djelatnicima.

Mnogi korisnici nemaju dovoljno znanja o prepoznavanju prijetnji i zaštiti digitalnih resursa.

PRISTUP EDUKACIJAMA

Ograničen pristup kvalitetnim edukacijskim sadržajima i nedostatak specijaliziranih programa otežavaju učinkovitu pripremu korisnika na stvarne kibernetičke napade.

Potreban je veći fokus na kontinuirano usavršavanje i prilagodbu edukacija suvremenim prijetnjama.



I Meet up: Dostupnost i teme edukacija o kibernetičkoj sigurnosti

Dostupnost edukacija

Edukacije su dostupne putem online platformi, radionica i seminara, no često imaju limitiran doseg u manjim institucijama i ruralnim područjima.

Ključne teme

- Tehničke teme
- Teme vezane za procese

Potencijal za razvoj

Potrebno je uvesti naprednije tematike poput obrane od naprednih prijetnji, enkripcije i forenzičke analize.



I Meet up: Financije

IZVORI FINANCIRANJA

Financijska sredstva dolaze iz državnih programa, europskih fondova te iz privatnog sektora.

Važan je pravilan raspored i transparentnost troškova kako bi ulaganja bila učinkovita.

PRIORITETI ULAGANJA

Prednost se daje **tehnologiji, edukaciji** zaposlenika i uspostavi sigurnosnih **procesa** unutar institucija.

Strategijsko financiranje omogućuje dugoročnu otpornost organizacija na kibernetičke prijetnje.

I **Meet up:** Za koje biste aktivnosti željeli dobiti financijsku podršku?

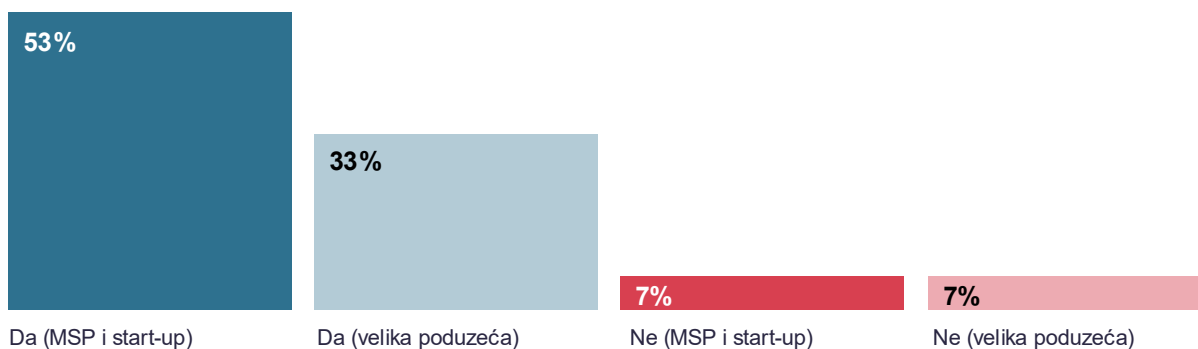
Značajan dio financijske potpore traži se za **edukacije zaposlenika, nabavu sigurnosne opreme te razvoj IT infrastrukture**. Također, važni su projekti za prevenciju i odgovor na kibernetičke napade.

Transparentno definirani **proces**i osiguravaju učinkovito usmjeravanje sredstava prema kritičnim područjima.

I Meet up: Dostatnost planiranog iznosa financiranja

Q

Maksimalni iznos financiranja je 60.000 eura. Smatrate li da je to dovoljno s obzirom na veličinu vašeg poduzeća ?





I Izazovi i očekivanja

Ključni izazovi

- Nedostatak specijaliziranih kadrova
- Brzi razvoj kibernetičkih prijetnji
- Ograničeni budžeti i resursi

Očekivanja

- Povećanje sigurnosne sposobnosti
- Bolja integracija edukacija u radne procese
- Jačanje suradnje između javnog i privatnog sektora

Poziv na dostavu projektnih prijedloga



I Predmet i cilj Poziva

PREDMET POZIVA je dodjela bespovratnih sredstava u svrhu unaprjeđenja kibernetičke sigurnosti mikro, malih i srednjih poduzeća.

CILJ POZIVA je povećanje broja mikro, malih i srednjih poduzeća s pripremljenim, uspostavljenim ili unaprijeđenim internim procesima te osnaženim kapacitetima zaposlenika u području kibernetičke sigurnosti.



I Prihvatljivi prijavitelji



Mikro, mala i srednja poduzeća



Poslovni nastan u Hrvatskoj



Ukupan iznos **Raspon financiranja**

1.970.000,00 EUR
nbespovratnih sredstava
na raspolaganju

Od 7.500,00 EUR do
60.000,00 EUR
bespovratnih sredstava
po projektu

Sufinanciranje

Stopa sufinanciranja iznosi 50%





| Prihvatljive aktivnosti

- Provođenje analize zrelosti kibernetičke sigurnosti i potrebe za uvođenjem određenih mjera
- Usklađivanje procesa, dokumentacije i implementacije mjera uključivo i certificiranje temeljem provedena analize zrelosti kibernetičke sigurnosti
- Edukacija u području kibernetičke sigurnosti
- Sigurnosna testiranja



Slijedeći koraci



Javno savjetovanje



Objava poziva



Evaluacija prijava



Ugovaranja



Provedba projekta



Važni datumi

OTVARANJE POZIVA	srpanj 2025.
ZATVARANJE POZIVA	listopad 2025.
UGOVARANJE	siječanj 2026.



www.nks.hr



info@nks.hr