AGENCIJA EUROPSKE UNIJE ZA KIBERSIGURNOST

# EUROPA POVJERENJA I KIBERSIGURNOSTI

## Strategija ENISA-e

lipanj 2020.

# EUROPA POVJERENJA I KIBERSIGURNOSTI

AGENCIJA EUROPSKE UNIJE ZA KIBERSIGURNOST

# PREDGOVOR

**Već više od 15 godina ENISA, Agencija Europske unije za kibersigurnost, ima ključnu ulogu u ostvarivanju ambicije EU-a da ojača povjerenje u digitalne tehnologije i sigurnost u cijeloj Europi uz potporu država članica te institucija i agencija EU-a. Pružajući potporu međusobnom povezivanju zajednica ENISA je pridonijela jačanju pripravnosti Europe i njezinih sposobnosti odgovora na kiberincidente.**

Istodobno je zabilježen drastičan porast digitalizacije našega gospodarstva i društva, na što je ukazala i kriza izazvana epidemijom bolesti COVID-19, tijekom koje se pokazalo da je kolektivan i masovan zaokret prema IT rješenjima za rad na daljinu bio od ključne važnosti za nastavak obavljanja mnogih djelatnosti. Ta je kriza ukazala na to do koje mjere kibernetički napadači mogu iskoristiti našu ovisnost o tim tehnologijama. Ujedno je postalo jasno da je došlo do proširenja okruženja kiberprijetnji, koje uz ciljane napade sada uključuju i nove oblike masovnih prijetnji milijunima poduzeća i građana, a porastao je i broj incidenata povezanih sa sofisticiranim ucjenjivačkim softverima (eng. ransomware). Ubrzan razvoj digitalnih proizvoda i usluga, od računalstva u oblaku i videokonferencija do mreže 5G i umjetne inteligencije, isto je tako donio nove probleme koje je potrebno otkriti i nadvladati.

U osvit nove ere kibersigurnosti u Europi, uz svoj trajni mandat te širi opseg zadaća i sposobnosti, ENISA sada više nego ikada prije treba preuzeti vodeću ulogu i pomoći EU-u i državama članicama da odgovore na te probleme.

Kako bi u tome uspjela, ENISA će nastojati predvidjeti relevantne trendove te doći do najsuvremenijih stručnih znanja koja su važna za sve i podijeliti ih s drugima. ENISA će pružati potporu Europskoj komisiji i državama članicama u njihovu nastojanju da pomognu javnim i privatnim subjektima i građanima da spriječe rizike povezane s kiberincidentima te da njima uspješno upravljaju. Provedbom okvira za kibersigurnosnu certifikaciju ENISA će pridonijeti promjeni paradigme tako što će povećati razinu sigurnosti digitalnih rješenja koja se primjenjuju u Europi. Na taj će način svima pomoći da budu sposobniji odabrati odgovarajuća rješenja i imaju više povjerenja u njih. Agencija će pružati i aktivnu potporu europskoj operativnoj zajednici u području kibersigurnosti kroz blisku suradnju i pripremu zajedničkih odgovora na sljedeći kiberincident velikih razmjera koji pogodi Europu.

U okviru ENISA-ine nove uloge, otvorenost, fleksibilnost i pouzdanost bit će ključni pokretači njezinih svakodnevnih djelatnosti, a usto će intenzivnije surađivati s državama članicama i Europskom komisijom na usklađivanju pristupa. ENISA će isto tako nastojati ublažiti svoj utjecaj na okoliš u kontekstu aktualne klimatske krize te će nastojati biti društveno odgovorna institucija i pružiti uključivo radno okruženje.

Ovim se strateškim dokumentom, koji je izrađen u okviru uključivog postupka suradnje cjelokupnog osoblja ENISA-e, članova Upravljačkog odbora i Savjetodavne skupine ENISA-e, postavljaju jasni ciljevi na kojima će se temeljiti rad ENISA-e u narednim godinama kako bi se moglo uspješno odgovoriti na mnoge izazove koji su pred nama.

U ime Upravljačkog odbora

**Jean-Baptiste Demaison**
Predsjednik Upravljačkog odbora

**Krzysztof Silicki**
Zamjenik predsjednika Upravljačkog odbora

# VIZIJA

**Europa povjerenja i kibersigurnosti**

# MISIJA

Misija je Agencije Europske unije za kibersigurnost (ENISA) postići visoku zajedničku razinu kibersigurnosti u cijeloj Uniji u suradnji sa širom zajednicom. Agencija to čini tako što djeluje kao centar za stručno znanje u području kibersigurnosti te prikupljanjem i pružanjem neovisnih i visokokvalitetnih tehničkih savjeta i potpore iz područja kibersigurnosti državama članicama i tijelima EU-a. Pridonosi izradi i provedbi kiberpolitika Unije.

Naš je cilj ojačati povjerenje u povezanom gospodarstvu, povećati otpornost infrastrukture i usluga Unije kao i povjerenje u njih te čuvati digitalnu sigurnost našeg društva i građana. Želimo biti agilna te ekološki i društveno odgovorna organizacija usmjerena na čovjeka.

# VRIJEDNOSTI

**Usmjerenost na zajednice**
ENISA surađuje s različitim zajednicama, uzimajući pritom u obzir njihove kompetencije i stručno znanje, uspostavlja sinergije i potiče povjerenje kako bi što uspješnije ostvarila svoju misiju.

**Izvrsnost**
ENISA teži najsuvremenijem stručnom znanju u svojem radu, pridržava se najviših standarda kvalitete u pogledu poslovanja te ocjenjuje svoju uspješnost u nastojanju da se kontinuirano usavršava primjenom inovacija i predviđanja.

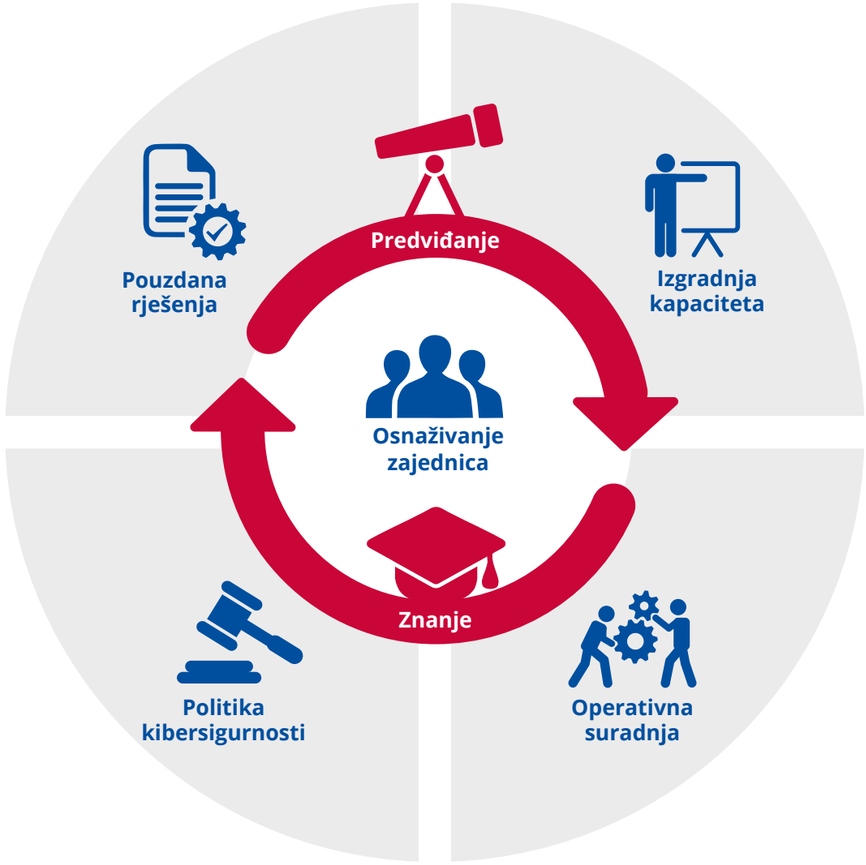
**Integritet/etičnost**
ENISA poštuje etička načela te se pridržava pravila i obveza relevantnih za EU u okviru svojih usluga i radnog okruženja, jamčeći na taj način pravednost i uključivost.

**Poštovanje**
ENISA je poštovanje temeljnih europskih prava i vrijednosti te očekivanja svojih dionika ugradila u sve svoje usluge i u čitavo radno okruženje.

**Odgovornost**
ENISA preuzima odgovornost i na taj način integrira društvene dimenzije i one koje se odnose na okoliš u prakse i postupke.

**Transparentnost**
ENISA primjenjuje postupke, strukture i procese koji su otvoreni, neovisni i utemeljeni na činjenicama te na taj način sprječava pristranost, dvosmislenost, prijevare i netransparentnost.

# STRATEŠKI CILJEVI



# SC1

## Strateški cilj

# OSNAŽENE I ANGAŽIRANE ZAJEDNICE U CIJELOM KIBERSIGURNOSNOM EKOSUSTAVU

## Kontekst

Kibersigurnost je zajednička odgovornost. Europa teži uspostavljanju međusektorskog i sveobuhvatnog okvira suradnje. ENISA ima ključnu ulogu kad je riječ o pokretanju aktivne suradnje među dionicima iz područja kibersigurnosti u državama članicama te institucijama i agencijama EU-a. Ona nastoji osigurati komplementarnost zajedničkih napora pružanjem dodane vrijednosti dionicima, istraživanjem mogućnosti sinergije i učinkovitom upotrebom ograničenog stručnog znanja i resursa iz područja kibersigurnosti. Zajednice je potrebno osnažiti kako bi mogle nadograđivati kibersigurnosni model.

## Što želimo postići

- najsuvremenijim se korpusom znanja na razini cijelog EU-a o konceptima i praksama iz područja kibersigurnosti, kojim se gradi suradnja među ključnim subjektima u području kibersigurnosti, promiču naučene lekcije i stručno znanje EU-a te stvaraju nove sinergije.
- osnaženi kibersigurnosni ekosustav koji obuhvaća tijela država članica, institucije, agencije i tijela EU-a, udruge, istraživačke centre i sveučilišta, industriju, privatne subjekte i građane, s obzirom na to da svi oni imaju važnu ulogu u osiguravanju kibersigurnosti Europe.

# SC2

Strateški cilj

# KIBERSIGURNOST KAO SASTAVNI DIO POLITIKA EU-A

## Kontekst

Kibersigurnost je okosnica digitalne transformacije i potreba za njom prožima sve sektore te ju je stoga potrebno uzeti u obzir u okviru širokog raspona područja i inicijativa politike. Kibersigurnost ne smije biti ograničena na usko specijaliziranu zajednicu tehničkih i kibernetičkih stručnjaka. To znači da kibersigurnost mora biti ugrađena u sve domene politike EU-a. Od ključne su važnosti izbjegavanje rascjepkanosti i potreba za koherentnim pristupom uz istodobno uzimanje u obzir posebnosti svakog sektora.

## Što želimo postići

- proaktivno savjetovanje i potporu za sve relevantne subjekte na razini EU-a, pri čemu se s pomoću izvedivih i ciljanih tehničkih smjernica unosi dimenzija kibersigurnosti u ciklus oblikovanja politika
- uspostavu okvira upravljanja kibersigurnosnim rizicima u svim sektorima i njihovo praćenje tijekom cijelog razdoblja primjene kibersigurnosne politike.

# SC3

Strateški cilj

# UČINKOVITA SURADNJA MEĐU OPERATIVNIM SUBJEKTIMA UNUTAR UNIJE U SLUČAJU MASOVNIH KIBERINCIDENATA

## Kontekst

Koristi europskog digitalnog gospodarstva i društva mogu se u potpunosti ostvariti jedino pod pretpostavkom kibersigurnosti. Kibernapadi ne poznaju granice. Svi slojevi društva mogu biti pogođeni te Unija mora biti spremna odgovoriti na masovne (velike i prekogranične) kibernapade i kiberkrize. Prekogranične međuovisnosti ukazale su na potrebu za učinkovitom suradnjom među državama članicama i institucijama EU-a kako bi se moglo brže odgovoriti na situaciju i pravilno koordinirati nastojanja na svim razinama (strateškoj, operativnoj, tehničkoj i komunikacijskoj).

## Što želimo postići

- kontinuiranu prekograničnu i višeslojnu potporu suradnji među državama članicama i institucijama EU-a posebno s obzirom na potencijalne incidente i krize velikih razmjera, pružanje potpore nadogradnji tehničke, operativne, političke i strateške suradnje među ključnim operativnim subjektima kako bi se omogućio pravodoban odgovor, razmjena informacija, informiranost o stanju i komunikacija u vezi s kriznim situacijama na razini cijele Unije
- sveobuhvatno i brzo tehničko rješavanje incidenata na zahtjev država članica kako bi se odgovorilo na tehničke i operativne potrebe u pogledu upravljanja incidentima i rizicima.

# SC4

## Strateški cilj

# VRHUNSKE KOMPETENCIJE I SPOSOBNOSTI U PODRUČJU KIBERSIGURNOSTI U CIJELOJ UNIJI

## Kontekst

Učestalost i sofisticiranost kibernapada ubrzano se povećava, a istodobno se sve veći broj pojedinaca, organizacija i industrija koristi infrastrukturama i tehnologijama IKT-a. Potražnja za znanjem i kompetencijama iz područja kibersigurnosti premašuje postojeću ponudu. EU mora ulagati u izgradnju kompetencija i vještina u području kibersigurnosti na svim razinama, od nestručnih radnika do visokokvalificiranih stručnjaka. Cilj ulaganja ne bi trebao biti samo povećati broj osoba s vještinama iz područja kibersigurnosti u državama članicama, već i osigurati da različite operativne zajednice posjeduju odgovarajuće kapacitete kako bi se mogle nositi s kiberprijetnjama.

## Što želimo postići

- usklađenost kompetencija, stručnog iskustva i obrazovnih struktura iz područja kibersigurnosti kako bi se zadovoljila sve veća potreba za znanjem i kompetencijama iz područja kibersigurnosti u EU-u;
- višu temeljnu razinu osviještenosti i kompetencija u pogledu kibersigurnosti u cijelom EU-u te uključivanje kiberpitanja u nove discipline;
- dobro usvojene i testirane sposobnosti uz prikladan kapacitet za suočavanje s okruženjem prijetnji koje se ubrzano razvija u cijelom EU-u.

# SC5

Strateški cilj

## VISOKA RAZINA POVJERENJA U SIGURNA DIGITALNA RJEŠENJA

## Kontekst

Digitalni proizvodi i usluge sa sobom nose koristi ali i rizike, a te je rizike potrebno prepoznati i ublažiti. U postupku ocjene sigurnosti digitalnih rješenja i osiguravanja njihove pouzdanosti od ključne je važnosti usvojiti zajednički pristup u svrhu postizanja ravnoteže u pogledu društvenih, tržišnih, gospodarskih i kibersigurnosnih potreba. Neutralan subjekt koji postupa transparentno povećat će povjerenje korisnika u digitalna rješenja te u šire digitalno okruženje.

## Što želimo postići

- kibersigurnost digitalnog okruženja u cijelom EU-u, u okviru kojeg građani mogu imati povjerenja u proizvode, usluge i postupke IKT-a zahvaljujući provedbi programa kibersigurnosne certifikacije u ključnim područjima tehnologije.

# SC6

Strateški cilj

# PREDVIĐANJE NOVIH I BUDUĆIH KIBERSIGURNOSNIH IZAZOVA

## Kontekst

Upotrebom metoda predviđanja pridonijelo bi se mnogim tehnologijama, bez obzira na to jesu li u ranoj fazi razvoja ili će uskoro biti službeno prihvaćene. Strukturiranim postupkom kojim se omogućuje dijalog među dionicima, donositelji odluka i oblikovatelji politika mogli bi utvrditi strategije ranog ublažavanja kojima bi se poboljšala otpornost EU-a na kibersigurnosne prijetnje i pronašla rješenja za svladavanje novih izazova.

## Što želimo postići

- razumijevanje novih trendova i obrazaca s pomoću predviđanja i budućih scenarija, čime će se pridonijeti ublažavanju kibersigurnosnih izazova s kojima se suočavaju naši dionici
- ranu ocjenu izazova i rizika koji proizlaze iz prilagodbe budućim trendovima i njihova prihvaćanja, uz ostvarivanje suradnje s dionicima u pogledu odgovarajućih strategija ublažavanja.

# SC7

Strateški cilj

# UČINKOVITO I DJELOTVORNO UPRAVLJANJEKIBERSIGURNOSNIM INFORMACIJAMA I ZNANJEM ZA EUROPU

## Kontekst

Energija koja pokreće koncept kibersigurnosti jesu informacije i znanje. Da bi stručnjaci iz područja kibersigurnosti mogli učinkovito postizati naše ciljeve, raditi u okruženju koje se neprestano mijenja – u smislu digitalnih promjena, ali i promjena u pogledu subjekata – te se suočavati s izazovima našeg vremena, potreban im je kontinuirani postupak prikupljanja, organiziranja, sažimanja, analiziranja i održavanja kibersigurnosnih informacija i znanja te komuniciranja o njima. Sve su faze od ključne važnosti kako bi se osigurala razmjena i širenje informacija i znanja u okviru kibersigurnosnog ekosustava EU-a.

## Što želimo postići

- upravljanje zajedničkim informacijama i znanjem za potrebe kibersigurnosnog ekosustava EU-a u pristupačnom, prilagođenom, pravodobnom i primjenjivom obliku, uz prikladnu metodologiju, infrastrukturu i alate u kombinaciji s metodama osiguranja kvalitete u svrhu kontinuiranog poboljšanja usluga.

## O ENISA-I

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije osnovana s ciljem postizanja visoke zajedničke razine kibersigurnosti u cijeloj Europi. Agencija Europske unije za kibersigurnost osnovana je 2004. na temelju Akta o kibersigurnosti EU-a i odonda pridonosi kiberpolitici EU-a, poboljšava pouzdanost proizvoda, usluga i postupaka IKT-a s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi na kiberizazove koji je očekuju u budućnosti. Razmjenom znanja, izgradnjom kapaciteta i informiranjem Agencija zajedno sa svojim ključnim dionicima radi na jačanju povjerenja u povezano gospodarstvo kako bi se povećala otpornost infrastrukture Unije te kako bi se u konačnici zaštitila sigurnost europskog društva i građana. Više informacija o ENISA-i i njezinu radu možete pronaći na www.enisa.europa.eu

TP-02-20-759-HR-N

**ENISA**
Agencija Europske unije za kibersigurnost

**Ured u Ateni**
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grčka

**Ured u Heraklionu**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grčka

enisa.europa.eu