AGENCIJA EVROPSKE UNIJE ZA KIBERNETSKO VARNOST

ZAUPANJA VREDNA IN KIBERNETSKO VARNA EVROPA

Strategija agencije ENISA

Junij 2020

ZAUPANJA VREDNA IN KIBERNETSKO VARNA EVROPA

AGENCIJA EVROPSKE UNIJE ZA KIBERNETSKO VARNOST

PREDGOVOR

Agencija EU za kibernetsko varnost (ENISA) ima že več kot 15 let ključno vlogo pri uresničevanju cilja EU, da se okrepita digitalno zaupanje in varnost po vsej Evropi, pri čemer sodeluje z državami članicami ter institucijami in agencijami EU. S povezovanjem skupnosti je uspešno prispevala k večji pripravljenosti in boljšim zmogljivostim Evrope za odzivanje na kibernetske incidente.

V tem času se je izrazito okrepila digitalizacija našega gospodarstva in družbe, kar se je pokazalo med krizo zaradi pandemije covida-19, ko smo vsi skupaj morali množično preiti na uporabo informacijskih rešitev na daljavo, da številne dejavnosti niso zastale. Med krizo je bilo vidno, kako zelo kibernetski napadalci izkoriščajo našo odvisnost od teh tehnologij. Pokazalo se je tudi, kako se je področje kibernetskih groženj razširilo, in sicer s ciljno usmerjenih napadov na nove oblike množičnih groženj več milijonom podjetij in državljanov, vključno z vse pogostejšimi tehnološko zapletenimi incidenti z izsiljevalskim programjem. S hitrim razvojem digitalnih proizvodov in storitev, od računalništva v oblaku in videokonferenc do tehnologije 5G in umetne inteligence, so se pojavili tudi novi izzivi, ki jih je treba še nadalje raziskati in najti rešitve zanje.

Agencija ENISA bo s svojim stalnim poslanstvom ter dodatnimi nalogami in zmogljivostmi bolj kot kdaj koli prej pripravljena na vodenje prizadevanj, ki bodo EU in njenim državam članicam pomagala pri odzivanju na te izzive, medtem ko se za kibernetsko varnost v Evropi začenja nova doba.

Agencija ENISA si bo v tem okviru prizadevala za napovedovanje pomembnih trendov ter zbirala in delila najnovejše strokovne izkušnje in znanje, da bodo na voljo vsem. Podpirala bo Evropsko komisijo in države članice pri ukrepih za pomoč javnim in zasebnim akterjem ter državljanom pri preprečevanju in obvladovanju tveganj, povezanih s kibernetskimi incidenti. Z izvajanjem certifikacijskega okvira za kibernetsko varnost bo prispevala k spremembi paradigme, saj bo izboljšala raven varnosti digitalnih rešitev, ki se uporabljajo v Evropi. S tem bo vsem povečala možnost izbire in pridobila njihovo zaupanje. Agencija bo tudi dejavno podpirala evropsko operativno skupnost na področju kibernetske varnosti pri tesnem sodelovanju in pripravah na skupen odziv, ko bo Evropo prizadel naslednji obsežen kibernetski incident.

Zdaj, ko agencija ENISA prevzema svojo novo vlogo, bodo ključni dejavniki pri njenem vsakodnevnem delovanju odprtost, okretnost in zanesljivost. Tesno bo sodelovala z državami članicami in Evropsko komisijo, da bodo uskladile pristope. Poleg tega si bo prizadevala, da bo izboljšala svoj vpliv na okolje, saj se svet trenutno spopada s podnebno krizo, ter da bo njeno delovno okolje družbeno odgovorno in vključujoče.

Ta strateški dokument, ki smo ga oblikovali v okviru vključujočega procesa sodelovanja vseh zaposlenih v agenciji ENISA ter članov upravnega odbora in svetovalne skupine, določa jasne cilje, ki bodo usmerjali delo agencije v prihodnjih letih, da bo lahko kos številnim izzivom, ki jo čakajo.

V imenu upravnega odbora

Jean-Baptiste Demaison
Predsednik upravnega odbora

Krzysztof Silicki
Namestnik predsednika upravnega odbora

VIZIJA

Zaupanja vredna in kibernetsko varna Evropa

POSLANSTVO

Poslanstvo Agencije Evropske unije za kibernetsko varnost (ENISA) je v sodelovanju s širšo skupnostjo doseči visoko skupno raven kibernetske varnosti po vsej Uniji. Za to si prizadeva z delovanjem v vlogi središča strokovnega znanja na področju kibernetske varnosti, ki zbira ter državam članicam in organom EU zagotavlja neodvisne kakovostne tehnične nasvete ter pomoč na tem področju. Agencija prispeva k oblikovanju in izvajanju kibernetskih politik Unije.

Njen cilj je okrepiti zaupanje v povezano gospodarstvo, povečati odpornost infrastrukture in služb Unije ter zaupanje vanje ter zagotavljati digitalno varnost naše družbe in državljanov. Stremi k temu, da bi bila prožna ter okoljsko in družbeno odgovorna organizacija, osredotočena na ljudi.

VREDNOTE

Usmerjenost v skupnost
Agencija ENISA sodeluje s skupnostmi, pri čemer spoštuje njihove sposobnosti in strokovno znanje, ter spodbuja sinergije in zaupanje, da bi kar najbolje opravila svoje poslanstvo.

Odličnost
Agencija ENISA si prizadeva, da pri svojem delu uporablja najnovejše strokovno znanje, ter deluje v skladu z najvišjimi standardi kakovosti in ocenjuje svojo uspešnost, s tem pa stremi k stalnemu izboljševanju na podlagi inovacij in predvidevanja.

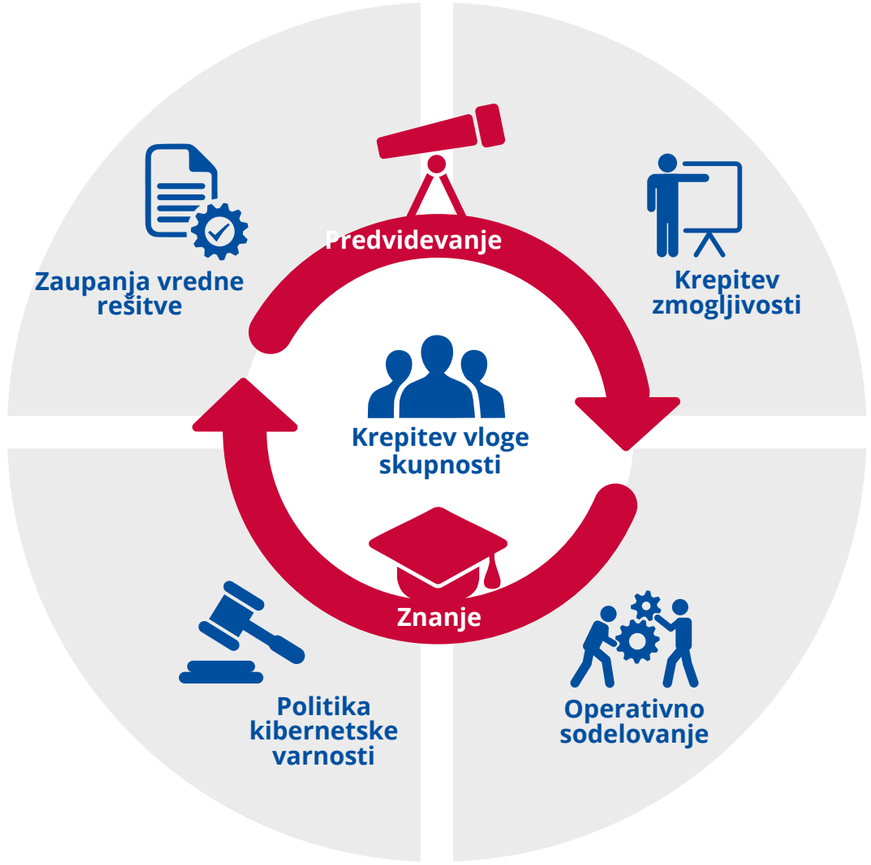
Integriteta in etika
Agencija ENISA pri svojih storitvah in v svojem delovnem okolju spoštuje etična načela ter pravila in obveznosti, ki veljajo v EU, s tem pa zagotavlja, da je pravična in vključujoča.

Spoštovanje
Agencija ENISA pri vseh svojih storitvah in v svojem delovnem okolju spoštuje temeljne evropske pravice in vrednote, pa tudi pričakovanja svojih deležnikov.

Odgovornost
Agencija ENISA prevzema odgovornost, s čimer zagotavlja vključevanje socialne in okoljske razsežnosti v prakse in postopke.

Preglednost
Agencija ENISA sprejema postopke, strukture in postopke, ki so odprti in neodvisni ter temeljijo na dejstvih, s čimer omejuje pristranskost, dvoumnost, goljufije in nejasnosti.

STRATEŠKI CILJI



SC1

Strateški cilj

OKREPLJENA VLOGA SKUPNOSTI IN NJIHOVO VKLJUČEVANJE V CELOTNEM EKOSISTEMU KIBERNETSKE VARNOSTI

Ozadje

Kibernetska varnost je naša skupna odgovornost. Evropa si prizadeva za medpanožni in vseobsegajoč okvir sodelovanja. Agencija ENISA ima ključno vlogo pri spodbujanju dejavnega sodelovanja med deležniki na področju kibernetske varnosti v državah članicah ter institucijah in agencijah EU. Stremi k temu, da bi se skupna prizadevanja dopolnjevala, in sicer s prinašanjem dodane vrednosti za deležnike, preučevanjem sinergij ter učinkovito uporabo omejenega strokovnega znanja in virov na področju kibernetske varnosti. Skupnostim bi bilo treba zagotoviti možnosti, da razširijo model kibernetske varnosti.

Kaj želimo doseči?

- Vseevropski korpus najnovejšega znanja o pojmih in praksah na področju kibernetske varnosti, ki bo vzpostavil sodelovanje med ključnimi akterji na tem področju, razširjal pridobljena spoznanja in strokovno znanje EU ter ustvarjal nove sinergije.
- Kibernetski ekosistem z okrepljeno vlogo, ki bo združeval organe držav članic, institucije, agencije in organe EU, združenja, raziskovalna središča in univerze, zasebnike in državljane, ki bodo omogočali, da je Evropa kibernetsko varna.

SC2

Strateški cilj

KIBERNETSKA VARNOST KOT SESTAVNI DEL POLITIK EU

Ozadje

Kibernetska varnost je temelj digitalne preobrazbe, saj potreba po njej pa prežema vse sektorje, zato jo je treba upoštevati pri najrazličnejših področjih politik in pobudah. Kibernetska varnost ne sme biti omejena na specializirano skupnost tehničnih kibernetskih strokovnjakov, zato jo je treba vključiti v vsa področja politike EU. Nujno je preprečevati razdrobljenost in zagotoviti usklajen pristop, pri tem pa upoštevati posebne značilnosti posameznega sektorja.

Kaj želimo doseči?

- Proaktivno svetovanje in podporo vsem zadevnim akterjem na ravni EU, ki razsežnost kibernetske varnosti vključujejo v cikel oblikovanja politik, z izvedljivimi in ciljno usmerjenimi tehničnimi smernicami.
- Okvire za obvladovanje tveganj na področju kibernetske varnosti, ki bodo vzpostavljeni v vseh sektorjih in se bodo upoštevali v celotnem ciklu politike kibernetske varnosti.

SC3

Strateški cilj

UČINKOVITO SODELOVANJE MED OPERATIVNIMI AKTERJI V UNIJI V PRIMERU MNOŽIČNIH KIBERNETSKIH INCIDENTOV

Ozadje

Koristi evropskega digitalnega gospodarstva in družbe je mogoče v celoti doseči le pod okriljem kibernetske varnosti. Kibernetski napadi se ne ustavijo na mejah. Prizadenejo lahko vse ravni družbe, zato mora biti Unija pripravljena na odziv na množične (obsežne in čezmejne) kibernetske napade in kibernetsko krizo. Čezmejna medsebojna odvisnost je pokazala, da je potrebno učinkovito sodelovanje med državami članicami in institucijami EU za hitrejše odzivanje in ustrezno usklajevanje prizadevanj na vseh ravneh (strateški, operativni, tehnični in komunikacijski).

Kaj želimo doseči?

- Stalno čezmejno podporo na vseh ravneh za sodelovanje med državami članicami ter z institucijami EU. Zlasti glede na morebitne obsežne incidente in krize, želimo zagotavljati podporo razširjanju tehničnega, operativnega, političnega in strateškega sodelovanja med ključnimi operativnimi akterji, da bi omogočili pravočasen odziv, izmenjavo informacij, spremljanje razmer in krizno komuniciranje v vsej Uniji.
- Celovito in hitro tehnično obravnavanje incidentov na zahtevo držav članic, da se bo lažje zadostilo tehničnim in operativnim potrebam pri obvladovanju incidentov in kriz.

SC4

Strateški cilj

VRHUNSKA ZNANJA IN SPOSOBNOSTI NA PODROČJU KIBERNETSKE VARNOSTI V VSEJ UNIJI

Ozadje

Pogostost in tehnološka zapletenost kibernetskih napadov se hitro povečujeta, obenem pa posamezniki, organizacije in industrija pospešeno vedno pogosteje uporabljajo infrastrukture in tehnologij IKT. Povpraševanje po znanju in kompetencah na področju kibernetske varnosti presega ponudbo. EU mora vlagati v razvoj kompetenc in talentov na področju kibernetske varnosti na vseh ravneh, od laičnih uporabnikov do visoko usposobljenih strokovnjakov. Naložbe ne bi smele biti usmerjene le v razširitev nabora znanj in spretnosti v državah članicah, temveč tudi v zagotavljanje, da bodo imele različne operativne skupnosti ustrezne zmogljivosti za spoprijemanje z različnimi kibernetskimi grožnjami.

Kaj želimo doseči?

- Usklajene kompetence, strokovne izkušnje in izobraževalne strukture na področju kibernetske varnosti, da bodo izpolnjene naraščajoče potrebe po znanju in kompetencah na tem področju v EU.
- Večjo osnovno raven ozaveščenosti o kibernetski varnosti in kompetenc na tem področju po vsej EU ob vključevanju kibernetske razsežnosti v nove discipline.
- Dobro pripravljene in preizkušene zmogljivosti za ustrezno spoprijemanje s spreminjajočimi grožnjami po vsej EU.

SC5

Strateški cilj

VISOKA RAVEN ZAUPANJA V VARNE DIGITALNE REŠITVE

Ozadje

Digitalni proizvodi in storitve poleg koristi prinašajo tudi tveganja, ki jih je treba ugotoviti in zmanjševati. Pri procesu ocenjevanja varnosti digitalnih storitev in zagotavljanja, da so zaupanja vredne, je bistveno sprejeti skupen pristop, da sprejmemo skupen pristop za dosego ravnovesja med potrebami, povezanimi z družbo, trgom, gospodarstvom in kibernetsko varnostjo. Nevtralen subjekt, ki bo deloval pregledno, bo povečal zaupanje potrošnikov v digitalne rešitve in širše digitalno okolje.

Kaj želimo doseči?

- Kibernetsko varno digitalno okolje v vsej EU, v katerem bodo državljani lahko zaupali proizvodom, storitvam in procesom IKT, ko bodo na ključnih tehnoloških področjih uvedene certifikacijske sheme.

SC6

Strateški cilj

PREDVIDEVANJE GLEDE NASTAJAJOČIH IN PRIHODNJIH IZZIVOV NA PODROČJU KIBERNETSKE VARNOSTI

Ozadje

Pri številnih novih tehnologijah, ki so še v povojih ali pa že blizu splošne uporabe, bi izkoristili metode predvidevanja. Nosilci odločanja in oblikovalci politik bi lahko s strukturiranim postopkom, ki bi omogočal dialog med različnimi deležniki, opredelili strategije za zgodnje blaženje nevarnosti, ki bi izboljšale odpornost EU na grožnje kibernetski varnosti ter zagotovile rešitve za nastajajoče izzive.

Kaj želimo doseči?

- Razumevanje nastajajočih trendov in vzorcev s predvidevanjem in scenariji za prihodnost, ki bodo prispevali k blaženju kibernetskih izzivov naših deležnikov.
- Zgodnje ocenjevanje izzivov in tveganj, povezanih s sprejemanjem nastajajočih prihodnjih možnosti in prilagajanjem nanje, ob hkratnem sodelovanju z deležniki glede ustreznih strategij za blaženje nevarnosti.

SC7

Strateški cilj

UČINKOVITO IN USPEŠNO UPRAVLJANJE INFORMACIJ IN ZNANJA ZA EVROPO

Ozadje

Delo na področju kibernetske varnosti temelji na informacijah in znanju. Da lahko strokovnjaki za kibernetsko varnost učinkovito uresničujemo svoje cilje, da lahko delamo v okolju, ki se stalno spreminja (z vidika digitalnega razvoja in z vidika akterjev), da se lahko spoprijemamo s sodobnimi izzivi, potrebujemo stalen proces zbiranja, organizacije, povzemanja, analiziranja, sporočanja in vzdrževanja informacij in znanja o kibernetski varnosti. Vse te faze so bistvene za zagotovitev, da se bodo informacije in znanje v ekosistemu kibernetske varnosti EU izmenjevali, njihov obseg pa povečeval.

Kaj želimo doseči?

- Skupno upravljanje informacij in znanja v ekosistemu kibernetske varnosti EU v dostopni, prilagojeni, pravočasni in uporabni obliki z ustrezno metodologijo, infrastrukturo in orodji ter skupaj z metodami za zagotavljanje kakovosti, da bomo storitve stalno izboljševali.

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost, ENISA, je agencija Unije, katere cilj je dosegati visoko skupno raven kibernetske varnosti po vsej Evropi. Ustanovljena je bila leta 2004, njene pristojnosti pa so bile okrepljene z uredbo EU o kibernetski varnosti. Prispeva h kibernetski politiki EU, povečuje zaupanje v produkte, storitve in procese IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi, da bo pripravljena na kibernetske izzive prihodnosti. Z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter na koncu zagotovila digitalno varnost evropske družbe in državljanov. Več informacij o agenciji ENISA in njenem delu je na voljo na naslovu www.enisa.europa.eu.

TP-02-20-759-SL-N

ENISA
Agencija Evropske unije za kibernetsko varnost

Pisarna v Atenah
1 Vasilissis Sofias
151 24 Marousi, Attiki, Grčija

Pisarna v Heraklionu
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grčija

enisa.europa.eu