



Odbor za unutarnje tržište i zaštitu potrošača

2017/0225(COD)

22.5.2018

MIŠLJENJE

Odbora za unutarnje tržište i zaštitu potrošača

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti“)
(COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Izvjestitelj za mišljenje: (*) Nicola Danti

(*) Pridruženi odbor – članak 54. Poslovnika

PA_Legam

KRATKO OBRAZLOŽENJE

U digitalnom dobu kibersigurnost je ključan element za gospodarsku konkurentnost i sigurnost Europske unije te za integritet naših slobodnih i demokratskih društava i procesa na kojima se temelje. Zajamčena visoka razina kiberotpornosti diljem EU-a iznimno je važna za postizanje povjerenja potrošača u jedinstveno digitalno tržište i za daljnji razvoj inovativnije i konkurentnije Europe.

Nema sumnje u to da su kiberprijetnje i globalni kibernapadi – kao što su „Wannacry” i „Meltdown” – pitanja od sve veće važnosti u našem u sve većoj mjeri digitaliziranom društvu. Prema ispitivanju Eurobarometra objavljenom u srpnju 2017., 87 % ispitanika smatra kiberkriminalitet „važnim izazovom za unutarnju sigurnost EU-a”, a većina njih „zabrinuta je da su žrtve raznih oblika kiberkriminaliteta”. Štoviše, od početka 2016. svaki dan diljem svijeta dogodilo se više od 4 000 napada ucjenjivačkim softverima, uz povećanje od 300 % od 2015. i s učinkom na 80 % trgovačkih društava iz EU-a. Ove činjenice i saznanja jasno ukazuju na potrebu da EU bude otporniji i učinkovitiji u borbi protiv kibernapada te da poveća svoje sposobnosti kako bi bolje zaštitio građane Europe, poduzeća i javne institucije.

Godinu dana nakon stupanja na snagu Direktive NIS Europska je komisija u širem okviru strategije EU-a za kibersigurnost predstavila uredbu kojoj je cilj dodatno povećanje otpornosti, odvraćanja i obrane EU-a u području kibersigurnosti. Dana 13. rujna 2017. Komisija je predstavila „Akt o kibersigurnosti” na osnovi dvaju stupova, kako slijedi:

1. trajan i snažniji mandat za Agenciju Europske unije za mrežnu i informacijsku sigurnost (ENISA) kako bi se pomoglo državama članicama u učinkovitom sprječavanju kibernapada i odgovoru na njih i 2. uspostava okvira EU-a za kibersigurnosnu certifikaciju kako bi se zajamčilo da su IKT proizvodi i usluge kibersigurni.

Općenito, izvjestitelj pozdravlja pristup koji predlaže Europska komisija i osobito podržava uvodenje programa kibersigurnosne certifikacije na razini EU-a, kojima je cilj jačanje sigurnosti IKT proizvoda i usluga i izbjegavanje skupe rascjepkanosti jedinstvenog tržišta u tom ključnom području. Iako bi to prvenstveno trebalo ostati dobrovoljan alat, izvjestitelj se nada da će okvir EU-a za kibersigurnosnu certifikaciju i srođni postupci postati nužan alat za jačanje povjerenja naših građana i korisnika te povećanje sigurnosti proizvoda i usluga koji se kreću na jedinstvenom tržištu.

Dakako, također je uvjeren da niz stavki prijedloga treba razjasniti i poboljšati:

- Prije svega, **više uključiti relevantne dionike u različite faze sustava upravljanja za pripremu ENISA-inih prijedloga programa kibersigurnosne certifikacije**: prema mišljenju izvjestitelja, nužno je formalno uključiti najrelevantnije dionike kao što su industrije IKT-a, organizacije potrošača, MSP-ovi, normizacijska tijela EU-a i sektorske agencije EU-a itd. i dati im mogućnost da podnose nove prijedloge programa, savjetuju ENISA-u svojim stručnim znanjem ili surađuju s ENISA-om u pripremi prijedloga programa.
- Kao drugo, postoji potreba za jačanjem koordinacijske uloge Europske skupine za kibersigurnosnu certifikaciju (sastavljene od nacionalnih tijela i s podrškom Komisije i ENISA-e) dodatnim zadacima da pruža strateško vođenje i **uspostavi program rada za zajedničko djelovanje koje treba poduzeti na razini Unije** u području certifikacije te da uspostavi i **periodički ažurira prioritetni popis IKT proizvoda i usluga** za koje smatra da im je potreban europski program kibersigurnosne certifikacije.

- Izvjestitelj čvrsto vjeruje da bismo trebali izbjegavati praksu traženja najpovoljnije certifikacije EU-a („shopping”), što se već dogodilo u drugim sektorima. Potrebno je **izrazito ojačati odredbe za praćenje i nadzor koje se odnose na ENISA-u i nacionalna tijela za nadzor certifikacije** kako bi se zajamčilo da europski certifikat izdan u jednoj državi članici ima iste standarde i zahtjeve kao i certifikat izdan u drugoj državi članici. Stoga predlaže:
 1. jačanje nadzornih ovlasti ENISA-e: ENISA bi trebala zajedno sa Skupinom za certifikaciju ocijeniti postupke koje su uspostavila tijela odgovorna za izdavanje certifikata EU-a;
 2. da nacionalna tijela za nadzor certifikacije provode periodička ocjenjivanja (barem svake dvije godine) certifikata EU-a koje su izdala tijela za ocjenjivanje sukladnosti;
 3. uvođenje zajedničkih obvezujućih kriterija koje će definirati Skupina kako bi se postavili razmjer, opseg i učestalost ocjenjivanja iz točke 2. koja će provoditi nacionalna tijela za nadzor certifikacije.
- Izvjestitelj smatra da bi trebalo uvesti obveznu **oznaku povjerenja EU-a** za certificirane IKT proizvode i usluge koji su namijenjeni krajnjim korisnicima. Ta bi oznaka pomogla u podizanju razine osviještenosti, a trgovačkim društvima s dobrim kibersigurnosnim certifikatima povećala bi konkurentnost.
- Izvjestitelj se slaže s jedinstvenim i usklađenim pristupom Komisije, ali stajališta je da bi trebao biti fleksibilniji i prilagodljiviji posebnim značajkama i slabostima svakog proizvoda i usluge umjesto primjene načela jedinstvenog pristupa. Stoga izvjestitelj smatra da je potrebno preimenovati **razine jamstva** i primjenjivati ih uzimajući u obzir i planiranu namjenu IKT proizvoda i usluga. Isto tako, trajanje **valjanosti certifikata** trebalo bi se definirati na osnovi pojedinačnog programa.
- Svaki program certifikacije trebao bi biti osmišljen tako da stimulira i potiče sve dionike uključene u predmetni sektor da razvijaju i usvajaju sigurnosne standarde, tehničke norme i **načela integrirane sigurnosti i integrirane privatnosti** u svim fazama životnog vijeka proizvoda ili usluge.

AMANDMANI

Odbor za unutarnje tržište i zaštitu potrošača poziva Odbor za industriju, istraživanje i energiju da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1

Prijedlog uredbe

Uvodna izjava 1.

Tekst koji je predložila Komisija

(1) Mrežni i informacijski sustavi i telekomunikacijske mreže i usluge imaju ključnu ulogu u društvu i postali su okosnica gospodarskog rasta. Informacijska i komunikacijska tehnologija podupire složene sustave kojima se podupiru društvene aktivnosti, osigurava neprekinuto funkcioniranje naših gospodarstava u ključnim sektorima poput zdravstva, energetike, financija i prometa te se posebno podupire funkcioniranje unutarnjeg tržišta.

Izmjena

(1) Mrežni i informacijski sustavi i telekomunikacijske mreže i usluge imaju ključnu ulogu u društvu i postali su okosnica gospodarskog rasta. Informacijska i komunikacijska tehnologija (**IKT**) podupire složene sustave kojima se podupiru **svakodnevne** društvene aktivnosti, osigurava neprekinuto funkcioniranje naših gospodarstava u ključnim sektorima poput zdravstva, energetike, financija i prometa te se posebno podupire funkcioniranje unutarnjeg tržišta.

Amandman 2

Prijedlog uredbe

Uvodna izjava 2.

Tekst koji je predložila Komisija

(2) Građani, poduzeća i javna tijela u cijeloj Uniji sada se koriste mrežnim i informacijskim sustavima. Digitalizacija i povezivost postaju ključne značajke sve većeg broja proizvoda i usluga, a uvođenjem interneta stvari očekuje se da će se u EU-u tijekom sljedećeg desetljeća upotrebljavati milijuni, ako ne i milijarde, povezanih digitalnih uređaja. Iako se na internet povezuje sve veći broj uređaja, sigurnost i otpornost **nisu** dostatno **ugrađeni u dizajn**, što dovodi do nedostatne kibersigurnosti. U tom kontekstu, zbog ograničene uporabe

Izmjena

(2) Građani, poduzeća i javna tijela u cijeloj Uniji sada se koriste mrežnim i informacijskim sustavima. Digitalizacija i povezivost postaju ključne značajke sve većeg broja proizvoda i usluga, a uvođenjem interneta stvari očekuje se da će se u EU-u tijekom sljedećeg desetljeća upotrebljavati milijuni, ako ne i milijarde, povezanih digitalnih uređaja. Iako se na internet povezuje sve veći broj uređaja, sigurnost i otpornost **ne ugrađuju se** dostatno **kao standardni element**, što dovodi do nedostatne kibersigurnosti. U tom kontekstu, zbog ograničene uporabe

certifikacije, organizacije i pojedinačni korisnici nemaju dovoljno informacija o kibersigurnosnim značajkama IKT proizvoda i usluga, što smanjuje povjerenje u digitalna rješenja.

certifikacije, organizacije i pojedinačni korisnici nemaju dovoljno informacija o kibersigurnosnim značajkama IKT proizvoda i usluga, što smanjuje povjerenje u digitalna rješenja *koje je nužno za uspostavu jedinstvenog digitalnog tržišta*.

Amandman 3

Prijedlog uredbe Uvodna izjava 3.

Tekst koji je predložila Komisija

(3) Rast digitalizacije i povezivosti donose veće kibersigurnosne rizike zbog čega je društvo u cjelini osjetljivije na prijetnje kibersigurnosti, a građani se suočavaju sa sve većim opasnostima, uključujući ranjive osobe kao što su djeca. Kako bi se *ublažio taj rizik* za društvo, treba poduzeti sve nužne mjere za poboljšanje *kibersigurnosti* u EU-u u cilju bolje zaštite mrežnih i informacijskih sustava, telekomunikacijskih mreža, digitalnih proizvoda, usluga i uređaja kojima se koriste građani, vlade i poduzeća, od MSP-ova do operatora ključnih infrastruktura, od kiberprijetnji.

Izmjena

(3) Rast digitalizacije i povezivosti donose *znatno* veće kibersigurnosne rizike zbog čega je društvo u cjelini osjetljivije na prijetnje kibersigurnosti, a građani se suočavaju sa sve većim opasnostima, uključujući ranjive osobe kao što su djeca. *Transformativnu moć umjetne inteligencije i strojnog učenja iskoristit će cijelo društvo, ali i kiberkriminalci*. Kako bi se *ublažili ti rizici* za društvo, treba poduzeti sve nužne mjere za poboljšanje *zaštite od kibernapada* u EU-u u cilju bolje zaštite mrežnih i informacijskih sustava, telekomunikacijskih mreža, digitalnih proizvoda, usluga i uređaja kojima se koriste građani, vlade i poduzeća, od MSP-ova do operatora ključnih infrastruktura, od kiberprijetnji.

Amandman 4

Prijedlog uredbe Uvodna izjava 4.

Tekst koji je predložila Komisija

(4) Kibernapadi su sve češći te je potrebna snažnija obrana povezanog gospodarstva i društva koje je osjetljivije na kiberprijetnje i napade. Međutim, iako su kibernapadi često prekogranični, politički odgovori nadležnih tijela za kibersigurnost i nadležnosti u području

Izmjena

(4) Kibernapadi su sve češći te je potrebna snažnija *i sigurnija* obrana povezanog gospodarstva i društva koje je osjetljivije na kiberprijetnje i napade. Međutim, iako su kibernapadi često prekogranični, politički odgovori nadležnih tijela za kibersigurnost i nadležnosti u

izvršavanja zakonodavstva uglavnom su nacionalne. Veliki kiberincidenti mogli bi uzrokovati prekid u opskrbi ključnim uslugama u cijelom EU-u. Zbog toga su potrebni učinkovit odgovor i upravljanje krizama na razini EU-a, koji se temelje na ciljanim politikama i opsežnijim instrumentima za europsku solidarnost i uzajamnu pomoć. Nadalje, za kreatore politike, industriju i korisnike stoga je važno redovito ocjenjivanje stanja kibersigurnosti i otpornosti u Uniji na temelju pouzdanih podataka Unije i sustavno predviđanje budućeg razvoja, izazova i opasnosti na razini Unije i na globalnoj razni.

području izvršavanja zakonodavstva uglavnom su nacionalne. Veliki kiberincidenti mogli bi uzrokovati prekid u opskrbi ključnim uslugama u cijelom EU-u. Zbog toga su potrebni učinkovit odgovor i upravljanje krizama na razini EU-a, koji se temelje na ciljanim politikama i opsežnijim instrumentima za europsku solidarnost i uzajamnu pomoć. Nadalje, za kreatore politike, industriju i korisnike stoga je važno redovito ocjenjivanje stanja kibersigurnosti i otpornosti u Uniji na temelju pouzdanih podataka Unije i sustavno predviđanje budućeg razvoja, izazova i opasnosti na razini Unije i na globalnoj razni.

Amandman 5

Prijedlog uredbe Uvodna izjava 5.

Tekst koji je predložila Komisija

(5) Zbog sve većih kibersigurnosnih izazova s kojima se Unija suočava potrebno je donijeti sveobuhvatan skup mjera koje bi se temeljile na prethodnom djelovanju Unije i kojima bi se poticali ciljevi koji se uzajamno podupiru. One uključuju potrebu za dalnjim povećanjem sposobnosti i spremnosti država članica i poduzeća te za poboljšanjem suradnje i **koordinacija** u državama članicama i institucijama, agencijama i tijelima EU-a. Nadalje, s obzirom na to da kiberprijetnje ne poznaju **granica**, trebalo bi povećati sposobnosti na razini Unije kojima bi se mogla dopuniti djelovanja država članica, posebno u slučaju velikih prekograničnih kiberprijetnji i kriza. Potrebno je uložiti dodatne napore u podizanje razine osviještenosti građana i poduzeća u području kibersigurnosti. Nadalje, povjerenje u jedinstveno digitalno tržište **trebalo** bi dodatno poboljšati ponudom transparentnih informacija o razini sigurnosti IKT proizvoda i usluga. To se

Izmjena

(5) Zbog sve većih kibersigurnosnih izazova s kojima se Unija suočava potrebno je donijeti sveobuhvatan skup mjera koje bi se temeljile na prethodnom djelovanju Unije i kojima bi se poticali ciljevi koji se uzajamno podupiru. One uključuju potrebu za dalnjim povećanjem sposobnosti i spremnosti država članica i poduzeća te za poboljšanjem suradnje i **koordinacije** u državama članicama i institucijama, agencijama i tijelima EU-a. Nadalje, s obzirom na to da kiberprijetnje ne poznaju **granice**, trebalo bi povećati sposobnosti na razini Unije kojima bi se mogla dopuniti djelovanja država članica, posebno u slučaju velikih prekograničnih kiberprijetnji i kriza. Potrebno je uložiti dodatne napore u podizanje razine osviještenosti građana i poduzeća u području kibersigurnosti. Nadalje, s **obzirom na to da kiberincidenti narušavaju** povjerenje u **pružatelje digitalnih usluga i** jedinstveno digitalno tržište **kao takvo, osobito među**

može olakšati certificiranjem na razini EU-a kojim će se osigurati zajednički kibersigurnosni zahtjevi i kriteriji za ocjenjivanje na svim nacionalnim tržištima i u svim sektorima.

potrošačima, povjerenje bi trebalo dodatno poboljšati ponudom transparentnih informacija o razini sigurnosti IKT proizvoda i usluga. To se može olakšati standardiziranim certificiranjem na razini EU-a, koje se temelji na europskim ili medunarodnim normama i kojim će se osigurati zajednički kibersigurnosni zahtjevi i kriteriji za ocjenjivanje na svim nacionalnim tržištima i u svim sektorima. Osim certifikacije na razini cijele Unije postoje niz dobrovoljnih mera koje sâm privatni sektor treba poduzeti za jačanje povjerenja u sigurnost IKT proizvoda i usluga, osobito u pogledu sve veće dostupnosti povezanih digitalnih uređaja. Na primjer, enkripcija i druge tehnologije za uspješno sprečavanje kibernapada, kao što je lanac blokova, trebali bi se učinkovitije upotrebljavati kako bi se poboljšala sigurnost komunikacije i podataka krajnjih korisnika te opća sigurnost mreža i informacijskih sustava u Uniji.

Amandman 6

Prijedlog uredbe Uvodna izjava 5.a (nova)

Tekst koji je predložila Komisija

Izmjena

(5a) Iako certifikacija i drugi oblici ocjenjivanja sukladnosti IKT proizvoda, usluga i postupaka imaju važnu ulogu, za poboljšanje kibersigurnosti potreban je višedimenzionalan pristup koji obuhvaća osobe, postupke i tehnologije. EU bi također trebao nastaviti snažno naglašavati i poticati druge napore, uključujući obrazovanje, osposobljavanje i razvoj vještina u području kibersigurnosti, podizanje razine osviještenosti na izvršnoj razini i razini uprave poduzeća, promicanje dobrovoljne razmjene informacija o kiberprijetnjama te zaokret s reaktivnog na proaktivni pristup za odgovor na prijetnje

*stavljanjem naglaska na sprečavanje
uspješnih kibernapada.*

Amandman 7

Prijedlog uredbe Uvodna izjava 7.

Tekst koji je predložila Komisija

(7) Unija je već poduzela važne korake kako bi osigurala kibersigurnost i povećala povjerenje u digitalne tehnologije. Tijekom 2013. donesena je Strategija EU-a za kibersigurnost kako bi se usmjerio politički odgovor Unije na kibersigurnosne prijetnje i rizike. U cilju bolje zaštite Europljana na internetu Unija je 2016. donijela prvi zakonodavni akt u području kibersigurnosti, Direktivu (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije („Direktiva NIS“). Direktivom NIS utvrđuju se zahtjevi u pogledu nacionalnih sposobnosti u području kibersigurnosti, uspostavljeni su prvi mehanizmi za jačanje strateške i operativne suradnje među državama članicama i uvedene su obveze u pogledu sigurnosnih mjera i obavijesti o incidentima u sektorima koji su od ključne važnosti za gospodarstvo i društvo, kao što su energetika, promet, vodoopskrba, bankarstvo, infrastruktura financijskog tržišta, zdravstvena skrb, digitalna infrastruktura i pružatelji ključnih digitalnih usluga (tražilice, usluge računalstva u oblaku i internetska tržišta). ENISA je dobila ključnu ulogu u podupiranju provedbe te Direktive. Nadalje, djelotvorna borba protiv kiberkriminaliteta važan je prioritet Europskog programa sigurnosti, čime se pridonosi općem cilju postizanja visoke razine kibersigurnosti.

Izmjena

(7) Unija je već poduzela važne korake kako bi osigurala kibersigurnost i povećala povjerenje u digitalne tehnologije. Tijekom 2013. donesena je Strategija EU-a za kibersigurnost kako bi se usmjerio politički odgovor Unije na kibersigurnosne prijetnje i rizike. U cilju bolje zaštite Europljana na internetu Unija je 2016. donijela prvi zakonodavni akt u području kibersigurnosti, Direktivu (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije („Direktiva NIS“). Direktivom NIS, *čiji će uspjeh uvelike ovisiti o učinkovitoj provedbi u državama članicama*, utvrđuju se zahtjevi u pogledu nacionalnih sposobnosti u području kibersigurnosti, uspostavljeni su prvi mehanizmi za jačanje strateške i operativne suradnje među državama članicama i uvedene su obveze u pogledu sigurnosnih mjera i obavijesti o incidentima u sektorima koji su od ključne važnosti za gospodarstvo i društvo, kao što su energetika, promet, vodoopskrba, bankarstvo, infrastruktura financijskog tržišta, zdravstvena skrb, digitalna infrastruktura i pružatelji ključnih digitalnih usluga (tražilice, usluge računalstva u oblaku i internetska tržišta). ENISA je dobila ključnu ulogu u podupiranju provedbe te Direktive. Nadalje, djelotvorna borba protiv kiberkriminaliteta važan je prioritet Europskog programa sigurnosti, čime se pridonosi općem cilju postizanja visoke razine kibersigurnosti.

Amandman 8

Prijedlog uredbe Uvodna izjava 11.

Tekst koji je predložila Komisija

(11) S obzirom na sve veće izazove kibersigurnosti s kojima se Unija suočava, trebalo bi povećati finansijske i ljudske resurse dodijeljene Agenciji u skladu s njezinom pojačanom ulogom i zadaćama i njezinom ključnom ulogom u ekosustavu organizacija koje brane europski digitalni ekosustav.

Izmjena

(11) S obzirom na sve veće *prijetnje i* izazove kibersigurnosti s kojima se Unija suočava, trebalo bi povećati finansijske i ljudske resurse dodijeljene Agenciji u skladu s njezinom pojačanom ulogom i zadaćama i njezinom ključnom ulogom u ekosustavu organizacija koje brane europski digitalni ekosustav.

Amandman 9

Prijedlog uredbe Uvodna izjava 28.

Tekst koji je predložila Komisija

(28) Agencija bi trebala pridonijeti podizanju razine osviještenosti javnosti o rizicima povezanim s kibersigurnošću i davati smjernice o dobroj praksi za pojedinačne korisnike koje su usmjerene na građane i organizacije. Agencija bi trebala pridonositi i promicanju najbolje prakse i *rješenja na razini građana i organizacija* prikupljanjem i analizom javno dostupnih informacija o znatnim incidentima i sastavljanjem izvješća u cilju pružanja smjernica poduzećima i građanima i poboljšanja opće razine pripravnosti i otpornosti. Agencija bi, nadalje, u suradnji s državama članicama i institucijama, tijelima, uredima i agencijama Unije trebala organizirati redovite kampanje informiranja i obrazovanja krajnjih korisnika s ciljem poticanja sigurnijeg ponašanja pojedinaca na internetu, podizanja razine osviještenosti o *potencijalnim opasnostima* u kiberprostoru, uključujući kiberkriminalitet

Izmjena

(28) Agencija bi trebala pridonijeti podizanju razine osviještenosti javnosti o rizicima povezanim s kibersigurnošću i davati smjernice o dobroj praksi za pojedinačne korisnike koje su usmjerene na građane i organizacije. Agencija bi trebala pridonositi i promicanju najbolje prakse *u pogledu kiberhigijene, odnosno jednostavne i rutinske mjere koje pojedinci i organizacije mogu poduzeti kako bi se opasnost od kiberprijetnji svela na najmanju moguću mjeru, kao što su višefaktorska autentifikacija, sigurnosni popravci, enkripcija i upravljanje pristupom. Trebala bi to činiti* prikupljanjem i analizom javno dostupnih informacija o znatnim incidentima *te* sastavljanjem i *objavljivanjem* izvješća i smjernica u cilju pružanja smjernica poduzećima i građanima i poboljšanja opće razine pripravnosti i otpornosti. Agencija bi, nadalje, u suradnji s državama članicama i institucijama, tijelima, uredima

kao što su phishing napadi, mreže zaraženih računala (botnet) te financijske i bankovne prijevare, i poticanja ***osnovnog*** savjetovanja o ***autentikaciji i zaštiti*** podataka. Agencija bi trebala imati glavnu ulogu u bržem osvješćivanju korisnika o sigurnosti uređaja.

i agencijama Unije trebala organizirati redovite kampanje informiranja i obrazovanja krajnjih korisnika s ciljem poticanja sigurnijeg ponašanja pojedinaca na internetu, podizanja razine osvještenosti o ***mjerama koje se mogu poduzeti radi zaštite od potencijalnih opasnosti*** u kiberprostoru, uključujući kiberkriminalitet kao što su phishing napadi, ***napadi ucjenjivačkim softverima, preuzimanje kontrole***, mreže zaraženih računala (botnet) te financijske i bankovne prijevare, i poticanja savjetovanja o ***osnovnoj višefaktorskoj autentifikaciji, enkripciji, sigurnosnim poporavcima, načelima upravljanja pristupom***, zaštiti podataka, i ***drugim tehnologijama za unaprjeđenje sigurnosti i privatnosti te o alatima za anonimizaciju***. Agencija bi trebala imati glavnu ulogu u bržem osvješćivanju korisnika o sigurnosti uređaja i ***sigurnom korištenju usluga, promicanju integrirane sigurnosti na razini Unije koja je izuzetno važna za sigurnost povezanih uređaja, osobito za ranjive krajnje korisnike koji uključuju djecu, te promicanju integrirane privatnosti***. Agencija bi trebala poticati sve krajnje korisnike da poduzmu odgovarajuće korake za sprečavanje i svodenje na najmanju moguću mjeru učinaka incidenata koji utječu na sigurnost njihovih mreža i informacijskih sustava. Trebalo bi uspostaviti partnerstva s akademskim ustanovama u kojima su pokrenute istraživačke inicijative u relevantnim područjima kibersigurnosti.

Amandman 10

Prijedlog uredbe Uvodna izjava 35.

Tekst koji je predložila Komisija

(35) Agencija bi trebala poticati države članice i pružatelje usluga da povećaju svoje opće sigurnosne standarde kako bi svi korisnici interneta mogli poduzeti

Izmjena

(35) Agencija bi trebala poticati države članice i pružatelje usluga da povećaju svoje opće sigurnosne standarde kako bi svi korisnici interneta mogli poduzeti

potrebne korake za osiguranje svoje osobne kibersigurnosti. Konkretno, pružatelji usluga i proizvođači proizvoda trebali bi povući ili reciklirati proizvode i usluge koji ne zadovoljavaju standarde kibersigurnosti. ENISA, u suradnji s nadležnim tijelima, može širiti informacije o razini kibersigurnosti proizvoda i usluga koje se nude na unutarnjem tržištu te pružateljima i proizvođačima izdavati upozorenja u kojima od njih traži da poboljšaju sigurnost, uključujući kibersigurnost, svojih proizvoda i **usluga**.

potrebne korake za osiguranje svoje osobne kibersigurnosti. Konkretno, pružatelji usluga i proizvođači proizvoda trebali bi povući ili reciklirati proizvode i usluge koji ne zadovoljavaju standarde kibersigurnosti. ENISA, u suradnji s nadležnim tijelima, može širiti informacije o razini kibersigurnosti proizvoda i usluga koje se nude na unutarnjem tržištu te pružateljima i proizvođačima izdavati upozorenja u kojima od njih traži da poboljšaju sigurnost, uključujući kibersigurnost, svojih proizvoda. **ENISA bi trebala objaviti takva upozorenja na web-mjestu namijenjenom pružanju informacija o programima certifikacije. Agencija bi trebala sastaviti smjernice o minimalnim sigurnosnim zahtjevima za informatičke uređaje koji se prodaju u Uniji ili izvoze iz nje. Takvim bi se smjernicama moglo pozvati proizvođače da dostave pisanu izjavu kojom se potvrđuje da uređaj ne sadržava hardver, softver ili ugrađene programe s poznatim sigurnosnim slabostima koje se mogu zloupotrijebiti, niti nepromjenjivu ili nekriptiranu lozinku ili pristupnu šifru koji ne prihvaćaju ažuriranja sigurnosne zaštite iz pouzdanih izvora koja su prikladno provjerena, da odgovor prodavača za predmetni uređaj obuhvaća odgovarajuću hijerarhiju pravnih likova i da prodavači obavještavaju krajnje korisnike kad će sigurnosna potpora za uređaj prestati.**

Amandman 11

Prijedlog uredbe Uvodna izjava 36.a (nova)

Tekst koji je predložila Komisija

Izmjena

(36 a) Norme su dobrovoljan i tržišno uvjetovan alat kojim se postavljaju tehnički zahtjevi i daju smjernice i koji proizlazi iz otvorenog, transparentnog i uključivog postupka. Primjena normi

olakšava usklađenost robe i usluga s pravom Unije te se njome podupiru europske politike sukladne Uredbi (EU) br. 1025/2012 o europskoj normizaciji. Agencija bi se trebala redovito savjetovati s europskim organizacijama za normizaciju i surađivati s njima, osobito kad priprema europske programe kibersigurnosne certifikacije.

Amandman 12

Prijedlog uredbe Uvodna izjava 44.

Tekst koji je predložila Komisija

(44) Agencija bi trebala imati Stalnu interesnu skupinu kao savjetodavno tijelo kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama. Stalna interesna skupina, koju na prijedlog izvršnog direktora osniva Upravljački odbor, trebala bi se usredotočiti na pitanja relevantna za dionike te bi trebala Agenciji skrenuti pozornost na njih. Sastav Stalne interesne skupine, s kojom se posebno treba savjetovati u pogledu nacrta programa rada, i **njezinim zadaćama trebao** bi osigurati **dostatnu** zastupljenost dionika u radu Agencije.

Izmjena

(44) Agencija bi trebala imati Stalnu interesnu skupinu kao savjetodavno tijelo kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača, **akademskom zajednicom** i drugim interesnim skupinama. Stalna interesna skupina, koju na prijedlog izvršnog direktora osniva Upravljački odbor, trebala bi se usredotočiti na pitanja relevantna za dionike te bi trebala Agenciji skrenuti pozornost na njih. **Kako bi se osigurala stvarna uključenost interesnih skupina u okvir kibersigurnosne certifikacije, Stalna interesna skupina trebala bi davati savjete i o tome koje bi IKT proizvode i usluge trebalo obuhvatiti budućim europskim programima kibersigurnosne certifikacije i trebala bi predložiti Komisiji da od Agencije zatraži pripremu prijedloga programa za takve IKT proizvode i usluge, bilo na vlastitu inicijativu ili nakon što relevantni dionici podnesu prijedloge.** Sastav Stalne interesne skupine, s kojom se posebno treba savjetovati u pogledu nacrta programa rada, i **njezine zadaće trebali** bi osigurati **efikasnu i pravednu** zastupljenost dionika u radu Agencije.

Amandman 13

**Prijedlog uredbe
Uvodna izjava 46.**

Tekst koji je predložila Komisija

(46) Kako bi se zajamčila potpuna autonomija i neovisnost Agencije i kako bi joj se omogućilo obavljanje dodatnih i novih zadaća, uključujući nepredviđene hitne zadaće, Agenciji bi trebalo osigurati dostatni i autonomni proračun s prihodima prvenstveno iz doprinosa Unije i doprinosa trećih zemalja koje sudjeluju u radu Agencije. Veći dio osoblja Agencija trebao bi izravno sudjelovati u operativnoj provedbi mandata Agencije. Državi članici domaćinu ili bilo kojoj drugoj državi članici trebalo bi omogućiti davanje dobrovoljnih doprinosa prihodima Agencije. Na subvencije koje se financiraju iz općeg proračuna Unije trebao bi se i dalje primjenjivati proračunski postupak Unije. Štoviše, Revizorski sud trebao bi provesti reviziju računa Agencije radi osiguranja transparentnosti *i odgovornosti*.

Izmjena

(46) Kako bi se zajamčila potpuna autonomija i neovisnost Agencije i kako bi joj se omogućilo obavljanje dodatnih i novih zadaća, uključujući nepredviđene hitne zadaće, Agenciji bi trebalo osigurati dostatni i autonomni proračun s prihodima prvenstveno iz doprinosa Unije i doprinosa trećih zemalja koje sudjeluju u radu Agencije. Veći dio osoblja Agencija trebao bi izravno sudjelovati u operativnoj provedbi mandata Agencije. Državi članici domaćinu ili bilo kojoj drugoj državi članici trebalo bi omogućiti davanje dobrovoljnih doprinosa prihodima Agencije. Na subvencije koje se financiraju iz općeg proračuna Unije trebao bi se i dalje primjenjivati proračunski postupak Unije. Štoviše, Revizorski sud trebao bi provesti reviziju računa Agencije radi osiguranja transparentnosti, *odgovornosti, djelotvornosti i učinkovitosti izdataka*.

Amandman 14

**Prijedlog uredbe
Uvodna izjava 47.**

Tekst koji je predložila Komisija

(47) Ocjenjivanje sukladnosti postupak je kojim se dokazuje da su ispunjeni određeni zahtjevi koji se odnose na proizvod, postupak, uslugu, sustav, osobu ili tijelo. Za potrebe ove Uredbe certifikacija bi se trebala smatrati vrstom ocjenjivanja sukladnosti u pogledu kibersigurnosnih značajki *proizvoda, postupka, usluge, sustava ili njihove kombinacije* („IKT proizvodi i usluge“) koju obavlja neovisna treća strana *koja nije proizvođač proizvoda ili pružatelj usluge*. Samom certifikacijom ne može se jamčiti kibersigurnost certificiranih IKT proizvoda

Izmjena

(47) Ocjenjivanje sukladnosti postupak je kojim se dokazuje da su ispunjeni određeni zahtjevi koji se odnose na proizvod, postupak, uslugu, sustav, osobu ili tijelo. Za potrebe ove Uredbe certifikacija bi se trebala smatrati vrstom ocjenjivanja sukladnosti u pogledu kibersigurnosnih značajki *i praksi uključenih u proizvod, postupak, uslugu, sustav ili njihovu kombinaciju* („IKT proizvodi i usluge“) koju obavlja neovisna treća strana *ili se provodi postupkom davanja vlastite izjave o sukladnosti*. Samom certifikacijom ne može se jamčiti

i usluga. Riječ je o postupku i tehničkoj metodologiji kojima se potvrđuje da su IKT proizvodi i usluge testirani i da su u skladu s određenim kibersigurnosnim zahtjevima koji su propisani drugdje, na primjer u tehničkim normama.

kibersigurnost certificiranih IKT proizvoda i usluga **te bi krajnjeg korisnika trebalo upoznati s time**. Riječ je o postupku i tehničkoj metodologiji kojima se potvrđuje da su IKT proizvodi i usluge **te postupci i sustavi na kojima se temelje** testirani i da su u skladu s određenim kibersigurnosnim zahtjevima koji su propisani drugdje, na primjer u tehničkim normama.

Amandman 15

Prijedlog uredbe Uvodna izjava 48.

Tekst koji je predložila Komisija

(48) **Kibersigurnosna** certifikacija ima **važnu** ulogu u jačanju povjerenja u IKT proizvode i usluge i njihovu sigurnost. Jedinstveno digitalno tržište, posebno podatkovno gospodarstvo i internet stvari, mogu se razvijati samo ako postoji opće povjerenje javnosti da se takvim proizvodima i uslugama osigurava **određena** razina kibersigurnosnog jamstva. Povezani i automatizirani automobili, elektronički medicinski proizvodi, industrijski automatizirani kontrolni sustavi ili pametne mreže samo su primjeri sektora u kojima se certificiranje već u velikoj mjeri primjenjuje ili će se vjerojatno primjenjivati u skoroj budućnosti. Kibersigurnosna certifikacija od ključne je važnosti u sektorima uređenima Direktivom NIS.

Izmjena

(48) **Europska kibersigurnosna** certifikacija ima **ključnu** ulogu u jačanju povjerenja u IKT proizvode i usluge i njihovu sigurnost. Jedinstveno digitalno tržište, posebno podatkovno gospodarstvo i internet stvari, mogu se razvijati samo ako postoji opće povjerenje javnosti da se takvim proizvodima i uslugama osigurava **visoka** razina kibersigurnosnog jamstva. Povezani i automatizirani automobili, elektronički medicinski proizvodi, industrijski automatizirani kontrolni sustavi ili pametne mreže samo su primjeri sektora u kojima se certificiranje već u velikoj mjeri primjenjuje ili će se vjerojatno primjenjivati u skoroj budućnosti. Kibersigurnosna certifikacija od ključne je važnosti u sektorima uređenima Direktivom NIS.

Amandman 16

Prijedlog uredbe Uvodna izjava 50.

Tekst koji je predložila Komisija

(50) Trenutačno se kibersigurnosna certifikacija IKT proizvoda i usluga provodi samo u ograničenoj mjeri. Ako

Izmjena

(50) Trenutačno se kibersigurnosna certifikacija IKT proizvoda i usluga provodi samo u ograničenoj mjeri. Ako

postoji, ona se većinom provodi na razini države članice ili u okviru programa industrijskih sektora. U tom kontekstu druge države članice u načelu ne priznaju certifikat koji je izdalo jedno nacionalno tijelo za kibersigurnost. Trgovačka društva stoga će možda morati certificirati svoje proizvode i usluge u nekoliko država članica u kojima djeluju, na primjer radi sudjelovanja u nacionalnim postupcima javne nabave. Nadalje, iako se javljaju novi programi, čini se da ne postoji usklađen i holistički pristup pitanjima horizontalne kibersigurnosti, na primjer u području interneta stvari. U postojećim programima postoje znatni nedostaci i razlike u pogledu opsega proizvoda, **razine** jamstva, materijalnih kriterija i stvarne upotrebe.

postoji, ona se većinom provodi na razini države članice ili u okviru programa industrijskih sektora. U tom kontekstu druge države članice u načelu ne priznaju certifikat koji je izdalo jedno nacionalno tijelo za kibersigurnost. Trgovačka društva stoga će možda morati certificirati svoje proizvode i usluge u nekoliko država članica u kojima djeluju, na primjer radi sudjelovanja u nacionalnim postupcima javne nabave, **što će povećati njihove troškove**. Nadalje, iako se javljaju novi programi, čini se da ne postoji usklađen i holistički pristup pitanjima horizontalne kibersigurnosti, na primjer u području interneta stvari. U postojećim programima postoje znatni nedostaci i razlike u pogledu opsega proizvoda, **razina** jamstva **utemeljenih na riziku**, materijalnih kriterija i stvarne upotrebe.

Amandman 17

Prijedlog uredbe Uvodna izjava 52.

Tekst koji je predložila Komisija

(52) S obzirom na navedeno nužno je uspostaviti europski okvir za kibersigurnosnu certifikaciju kojim se utvrđuju glavni horizontalni zahtjevi za buduće europske programe kibersigurnosne certifikacije koji omogućuju priznavanje i uporabu certifikata IKT proizvoda i usluga u svim državama članicama. Europski okvir trebao bi imati dvostruku svrhu: s jedne strane njime bi se trebalo pridonijeti povećanju povjerenja u IKT proizvode i usluge koji su certificirani u skladu s tim programima. S druge strane, njime bi se trebalo izbjegći umnožavanje proturječnih ili preklapajućih nacionalnih kibersigurnosnih certifikacija i tako smanjiti troškovi poduzećima koja djeluju na jedinstvenom digitalnom tržištu. Programi certificiranja trebali bi biti nediskriminirajući i temeljiti se na

Izmjena

(52) S obzirom na navedeno nužno je **usvojiti zajednički pristup i** uspostaviti europski okvir za kibersigurnosnu certifikaciju kojim se utvrđuju glavni horizontalni zahtjevi za buduće europske programe kibersigurnosne certifikacije koji omogućuju priznavanje i uporabu certifikata IKT proizvoda i usluga u svim državama članicama. **Pritom je ključno nadovezati se na postojeće nacionalne i međunarodne programe i sustave uzajamnog priznavanja, osobito Skupinu viših dužnosnika za sigurnost informacijskih sustava (SOG-IS), te omogućiti neometan prijelaz iz postojećih programa u takvim sustavima na programe u novom europskom okviru.** Europski okvir trebao bi imati dvostruku svrhu: s jedne strane njime bi se trebalo pridonijeti povećanju povjerenja u IKT

međunarodnim normama ili normama Unije, osim ako su te norme neučinkovite ili neprimjerene za ispunjavanje zakonitih ciljeva EU-a u tom pogledu.

proizvode i usluge koji su certificirani u skladu s tim programima. S druge strane, njime bi se trebalo izbjegići umnožavanje proturječnih ili preklapajućih nacionalnih kibersigurnosnih certifikacija i tako smanjiti troškovi poduzećima koja djeluju na jedinstvenom digitalnom tržištu. *Ako je europski program kibersigurnosne certifikacije zamijenio nacionalni program, certifikati izdani u okviru europskog programa trebali bi se prihvaćati kao valjani u slučajevima u kojima je potrebna certifikacija na temelju nacionalnog programa.* Programi certificiranja trebali bi se voditi integriranim sigurnošću i načelima iz Uredbe (EU) 2016/679. Trebali bi također biti nediskriminirajući i temeljiti se na međunarodnim normama ili normama Unije, osim ako su te norme neučinkovite ili neprimjerene za ispunjavanje zakonitih ciljeva EU-a u tom pogledu.

Amandman 18

Prijedlog uredbe Uvodna izjava 52.a (nova)

Tekst koji je predložila Komisija

Izmjena

(52a) *Europski okvir za kibersigurnosnu certifikaciju treba na ujednačen način uspostaviti u svim državama članicama kako bi se izbjegla praksa „traženja povoljnije certifikacije” zbog razlika u troškovima ili razini zahtjevnosti među državama članicama.*

Amandman 19

Prijedlog uredbe Uvodna izjava 55.

Tekst koji je predložila Komisija

Izmjena

(55) Europskim programima kibersigurnosne certifikacije trebalo bi se

(55) Europskim programima kibersigurnosne certifikacije trebalo bi se

osigurati da proizvodi i usluge koji su certificirani u skladu s **takvim** programom zadovoljavaju određene zahtjeve. Ti zahtjevi odnose se na mogućnost odupiranja, na određenoj razini jamstva, djelovanjima kojima bi se mogla ugroziti dostupnost, izvornost, cjevitost ili povjerljivost pohranjenih, poslanih ili obrađenih podataka ili povezanih funkcija ili usluge koje se nude s pomoću tih **proizvoda, postupaka**, usluga i sustava ili kojima se s pomoću njih može pristupiti u smislu ove Uredbe. U ovoj Uredbi ne mogu se podrobno utvrditi kibersigurnosni zahtjevi povezani sa svim IKT proizvodima i uslugama. IKT proizvodi i usluge i povezane kibersigurnosne potrebe toliko su različiti da je teško osmisiliti opće kibersigurnosne zahtjeve koji se mogu svuda primjenjivati. Stoga je za potrebe certifikacije potrebno prihvatiti širok i općenit pojam kibersigurnosti dopunjen skupom kibersigurnosnih ciljeva koje treba uzeti u obzir pri izradi europskih programa kibersigurnosne certifikacije. Načina postizanja tih ciljeva u određenim IKT proizvodima i uslugama trebalo bi potom podrobnije opisati na razini pojedinačnog programa certificiranja kojeg je donijela Komisija, na primjer upućivanjem na norme ili tehničke specifikacije.

*doprinijeti visokoj razini zaštite krajnjih korisnika i europskoj konkurentnosti te povećati razinu sigurnosti unutar jedinstvenog digitalnog tržišta, a konkretnije osigurati da IKT proizvodi i usluge koji su certificirani u skladu s nekim programom zadovoljavaju određene zahtjeve. Ti zahtjevi odnose se na mogućnost odupiranja, na određenoj razini jamstva, djelovanjima kojima bi se mogla ugroziti dostupnost, izvornost, cjevitost ili povjerljivost pohranjenih, poslanih ili obrađenih podataka ili povezanih funkcija ili usluge koje se nude s pomoću tih postupaka, proizvoda, usluga i sustava ili kojima se s pomoću njih može pristupiti u smislu ove Uredbe. U ovoj Uredbi ne mogu se podrobno utvrditi kibersigurnosni zahtjevi povezani sa svim IKT proizvodima i uslugama. IKT proizvodi i usluge i povezane kibersigurnosne potrebe toliko su različiti da je teško osmisiliti opće kibersigurnosne zahtjeve koji se mogu svuda primjenjivati. Stoga je za potrebe certifikacije potrebno prihvatiti širok i općenit pojam kibersigurnosti dopunjen skupom kibersigurnosnih ciljeva koje treba uzeti u obzir pri izradi europskih programa kibersigurnosne certifikacije. Načina postizanja tih ciljeva u određenim IKT proizvodima i uslugama trebalo bi potom podrobnije opisati na razini pojedinačnog programa certificiranja kojeg je donijela Komisija, na primjer upućivanjem na norme ili tehničke specifikacije. **Iznimno je važno da svaki europski program kibersigurnosne certifikacije bude osmišljen tako da stimulira i potiče sve dionike uključene u predmetni sektor da razvijaju i usvajaju sigurnosne standarde, tehničke norme i načela integrirane sigurnosti u svim fazama životnog vijeka proizvoda ili usluge. Ako su programom predviđene oznake ili znakovi, potrebno je nавести uvjete pod kojim se te oznake ili znakovi mogu upotrebljavati. Na tom znaku, koji bi mogao biti u obliku digitalnog logotipa ili koda QR, navodili bi se rizici povezani s radom i uprebom***

IKT proizvoda ili usluga te bi on trebao biti jasan i lako razumljivi za krajnjeg korisnika.

Amandman 20

Prijedlog uredbe

Uvodna izjava 55.a (nova)

Tekst koji je predložila Komisija

Izmjena

(55a) U svjetlu razvoja inovacija te sve veće dostupnosti i stalno rastućeg broja povezanih digitalnih uređaja u svim sektorima društva, osobita pozornost mora se posvetiti sigurnosti svih, pa čak i najjednostavnijih povezanih digitalnih uređaja. Budući da je certifikacija ključna metoda za povećanje povjerenja u tržište te veću sigurnost i otpornost, naglasak bi se stoga u novom okviru EU-a za kibersigurnosnu certifikaciju trebao staviti na povezane digitalne uređaje i usluge kako bi postali manje osjetljivi i sigurniji za potrošače i poduzeća.

Amandman 21

Prijedlog uredbe

Uvodna izjava 56.

Tekst koji je predložila Komisija

Izmjena

(56) Komisija bi trebala imati ovlasti zatražiti od ENISA-e da izradi prijedloge programa za određene IKT proizvode ili usluge. Komisija bi na temelju prijedloga programa koji je predložila ENISA trebala imati ovlasti donijeti europski program kibersigurnosne certifikacije s pomoću provedbenih akata. Uzimajući u obzir opću svrhu i sigurnosne ciljeve utvrđene u ovoj Uredbi, u europskim programima kibersigurnosne certifikacije koje donosi Komisija trebalo bi odrediti minimalni skup elemenata koji se odnose na predmet, područje primjene i

(56) ENISA bi trebala održavati namjensko web-mjesto s mrežno dostupnim alatom, jednostavnim za korištenje i koji prikazuje popis informacija o usvojenim programima, predloženim programima i programima koje je zatražila Komisija. Uzimajući u obzir opću svrhu i sigurnosne ciljeve utvrđene u ovoj Uredbi, u europskim programima kibersigurnosne certifikacije koje donosi Komisija trebalo bi odrediti minimalni skup elemenata koji se odnose na predmet, područje primjene i funkcioniranje pojedinačnog programa.

funkcioniranje pojedinačnog programa. Oni bi trebali uključivati, među ostalim, područje primjene i cilj kibersigurnosne certifikacije, uključujući kategorije obuhvaćenih IKT proizvoda i usluga, detaljnu specifikaciju kibersigurnosnih zahtjeva, na primjer upućivanjem na norme ili tehničke specifikacije, posebne kriterije i metode ocjenjivanja i predviđenu razinu jamstva: *osnovna, znatna i/ili visoka*.

Oni bi trebali uključivati, među ostalim, područje primjene i cilj kibersigurnosne certifikacije, uključujući kategorije obuhvaćenih IKT proizvoda i usluga, detaljnu specifikaciju kibersigurnosnih zahtjeva, na primjer upućivanjem na norme ili tehničke specifikacije, posebne kriterije i metode ocjenjivanja *povezane s radom i primjenom IKT proizvoda, postupka ili usluge, njihov inherentan rizik* i predviđenu razinu jamstva: *funkcionalno sigurnu, odnosno razine jamstva koje imaju funkcionalan stupanj sigurnosti, znatno sigurnu, vrlo sigurnu ili bilo koju kombinaciju tih razina. Razinama jamstva ne bi se trebala sugerirati absolutna sigurnost kako se krajnjeg korisnika ne bi dovelo u zabludu. Pozornost bi trebalo posvetiti i cijelom životnom ciklusu proizvoda. Kako bi se razjasnilo kojim će se rizicima određeni proizvod ili usluga moći oduprijeti zahvaljujući svojem dizajnu, ENISA bi trebala koordinirati izradu kontrolnog popisa rizika za koje se očekuje da se IKT postupak, proizvod ili usluga s njima suoče, prema određenoj kategoriji korisnika u nekom okruženju.*

Amandman 22

Prijedlog uredbe Uvodna izjava 56.a (nova)

Tekst koji je predložila Komisija

Izmjena

(56 a) Komisija bi trebala imati ovlasti zatražiti od ENISA-e da izradi prijedloge programa za određene IKT proizvode ili usluge. Komisiji treba delegirati ovlast za donošenje akata u skladu s člankom 290. Ugovora o funkcioniranju Europske unije u vezi s uspostavom europskog programa kibersigurnosne certifikacije za IKT proizvode i usluge. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s

*načelima utvrđenima u
Međuinsticijском sporazumu o boljoj
izradi zakonodavstva od 13. travnja 2016.
Posebno, s ciljem osiguravanja
ravnopravnog sudjelovanja u pripremi
delegiranih akata, Europski parlament i
Vijeće primaju sve dokumente istodobno
kada i stručnjaci iz država članica te
njihovi stručnjaci sustavno imaju pristup
sastancima stručnih skupina Komisije
koji se odnose na pripremu delegiranih
akata. Pri donošenju tih delegiranih akata
Komisija bi programe kibersigurnosne
certifikacije za IKT proizvode i usluge
trebala temeljiti na svim relevantnim
prijetlozima programa koje je predložila
ENISA kako bi učvrstilo povjerenje u
okvir za kibersigurnosnu certifikaciju i
njegovu predvidljivost te povećala razina
javne osvještenosti o njemu.*

Amandman 23

Prijedlog uredbe Uvodna izjava 56.b (nova)

Tekst koji je predložila Komisija

Izmjena

*(56b) Među metodama ocjenjivanja i
postupcima procjene povezanim s
europskim programom kibersigurnosne
certifikacije trebalo bi na razini Unije
promicati etičko hakiranje, čiji je cilj
lociranje slabosti i osjetljivosti uređaja i
informatickih sustava predviđanjem
planiranih akcija i vještina zlonamjernih
hakera.*

Amandman 24

Prijedlog uredbe Uvodna izjava 58.

Tekst koji je predložila Komisija

Izmjena

(58) Nakon donošenja europskog
programa kibersigurnosne certifikacije,

(58) Nakon donošenja europskog
programa kibersigurnosne certifikacije,

proizvođači IKT proizvoda ili pružatelji IKT usluga moći će podnijeti zahtjev za certifikaciju svojih proizvoda *i* usluga tijelu za ocjenjivanje sukladnosti po svojem izboru. Tijela za ocjenjivanje sukladnosti trebalo bi akreditirati akreditacijsko tijelo ako ispunjavaju određene zahtjeve propisane ovom Uredbom. Akreditacija bi se trebala izdavati na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve. Akreditacijska tijela trebala bi ukinuti akreditaciju tijela za ocjenjivanje sukladnosti ako ono ne ispunjava uvjete za akreditaciju, ili ih je prestalo ispunjavati, ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.

proizvođači IKT proizvoda ili pružatelji IKT usluga moći će podnijeti zahtjev za certifikaciju svojih *postupaka*, proizvoda *ili* usluga tijelu za ocjenjivanje sukladnosti po svojem izboru *ili sami dati izjavu da su njihovi proizvodi ili usluge sukladni s relevantnim europskim programom kibersigurnosne certifikacije*. Tijela za ocjenjivanje sukladnosti trebalo bi akreditirati akreditacijsko tijelo ako ispunjavaju određene zahtjeve propisane ovom Uredbom. Akreditacija bi se trebala izdavati na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve. Akreditacijska tijela trebala bi ukinuti akreditaciju tijela za ocjenjivanje sukladnosti ako ono ne ispunjava uvjete za akreditaciju, ili ih je prestalo ispunjavati, ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.
Kako bi se zajamčilo da se akreditacija provodi jednakom diljem Europske unije, nacionalna tijela za nadzor certifikacije trebala bi podlijetegati istorazinskoj stručnoj ocjeni kada je riječ o postupcima za provjeru sukladnosti proizvoda koji podliježu certificiranju u području kibersigurnosti.

Amandman 25

Prijedlog uredbe Uvodna izjava 59.

Tekst koji je predložila Komisija

(59) Od svih država članica treba tražiti da imenuju jedno tijelo za nadzor kibersigurnosne certifikacije koje će nadzirati usklađenost tijela za ocjenjivanje sukladnosti i certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovom državnom području sa zahtjevima iz ove Uredbe i s relevantnim programima kibersigurnosne certifikacije. Nacionalna tijela za nadzor certifikacije trebala bi rješavati pritužbe

Izmjena

(59) Od svih država članica treba tražiti da imenuju jedno tijelo za nadzor kibersigurnosne certifikacije koje će nadzirati usklađenost tijela za ocjenjivanje sukladnosti i certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovom državnom području sa zahtjevima iz ove Uredbe i s relevantnim programima kibersigurnosne certifikacije. Nacionalna tijela za nadzor certifikacije trebala bi rješavati pritužbe

fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovu državnom području, u prikladnoj mjeri istražiti predmet pritužbe i u razumnom roku obavijestiti podnositelja pritužbe o napretku i rezultatu istrage. Nadalje, ona bi trebala surađivati s drugim nacionalnim tijelima za nadzor certifikacije ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim programima kibersigurnosne certifikacije.

fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovu državnom području, u prikladnoj mjeri istražiti predmet pritužbe i u razumnom roku obavijestiti podnositelja pritužbe o napretku i rezultatu istrage. Nadalje, ona bi trebala surađivati s drugim nacionalnim tijelima za nadzor certifikacije ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim programima kibersigurnosne certifikacije. *Nadalje bi trebala nadzirati i provjeravati sukladnost vlastitih izjava o sukladnosti, kao i to jesu li europske kibersigurnosne certifikate izdala tijela za ocjenjivanje sukladnosti prema zahtjevima iz ove Uredbe, uključujući pravila koja je usvojila Europska skupina za kibersigurnosnu certifikaciju i zahtjeve odgovarajućeg europskog programa kibersigurnosne certifikacije. Učinkovita suradnja nacionalnih tijela za nadzor certifikacije ključna je za ispravnu provedbu europskih programa za kibersigurnosnu certifikaciju i tehničkih pitanja koja se odnose na kibersigurnost IKT proizvoda i usluga. Komisija bi trebala olakšati tu razmjenu informacija stavljanjem na raspolaganje općeg elektroničko-informacijskog sustava podrške, primjerice postojećeg Informacijskog i komunikacijskog sustava za tržišni nadzor (ICSMS) i Sustava brzog uzbunjivanja za opasne neprehrambene proizvode (RAPEX) kojima se koriste tijela za nadzor tržišta u skladu s Uredbom (EZ) br. 765/2008.*

Amandman 26

Prijedlog uredbe Uvodna izjava 63.

Tekst koji je predložila Komisija

Izmjena

(63) *Kako bi se dodatno utvrdili kriteriji za akreditaciju tijela za ocjenjivanje sukladnosti, ovlast donošenja akata u skladu s člankom 290. Ugovora o funkcioniranju Europske unije treba prenijeti na Komisiju. Komisija bi tijekom svojeg pripremnog rada trebala provoditi odgovarajuća savjetovanja, uključujući i savjetovanje sa stručnjacima.*
Savjetovanja bi trebalo provoditi u skladu s načelima propisanima u Međuinstитucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.
Kako bi se osiguralo ravnopravno sudjelovanje u izradi delegiranih akata, Europski parlament i Komisija trebali bi sve dokumente zaprimiti istodobno kada i stručnjaci država članica, a njihovi stručnjaci trebali bi sustavno imati pristup sastancima skupina stručnjaka Komisije koje se bave izradom delegiranih akata.

deleted

Amandman 27

Prijedlog uredbe Uvodna izjava 65.

Tekst koji je predložila Komisija

Izmjena

(65) Postupak ispitivanja trebao bi se koristiti za donošenje provedbenih akata o europskim programima kibersigurnosne certifikacije za IKT proizvode i usluge; o načinima provođenja istraživačke Agencije te o okolnostima, formatima i postupcima u skladu s kojima nacionalna tijela za nadzor certifikacije Komisiji dostavljaju obavijesti o akreditiranim tijelima za ocjenjivanje sukladnosti.

(65) Postupak ispitivanja trebao bi se koristiti za donošenje provedbenih akata o europskim programima kibersigurnosne certifikacije za IKT *postupke*, proizvode i usluge; o načinima provođenja istraživačke Agencije te o okolnostima, formatima i postupcima u skladu s kojima nacionalna tijela za nadzor certifikacije Komisiji dostavljaju obavijesti o akreditiranim tijelima za ocjenjivanje sukladnosti, *uzimajući u obzir dokazanu djelotvornost alata za elektroničko prijavljivanje „Informacijski sustav prijavljenih i imenovanih tijela prema novom pristupu“ (NANDO).*

Amandman 28

Prijedlog uredbe Uvodna izjava 66.

Tekst koji je predložila Komisija

(66) Rad Agencije trebao bi se ocjenjivati neovisno. *Ocjenvanjem* bi trebalo *uzeti u obzir ostvaruje li* Agencija *svoje ciljeve, njezin način rada i relevantnost njezinih zadaća.* Ocjenjivanjem bi trebalo procijeniti i učinak, djelotvornost i učinkovitost europskog okvira za kibersigurnosno certificiranje.

Izmjena

(66) Rad Agencije trebao bi se ocjenjivati neovisno. *Ocjenvanje* bi trebalo *obuhvaćati ispravnost i učinkovitost načina na koji* Agencija *troši sredstva, njezinu djelotvornost u ostvarivanju ciljeva te opis njezina načina rada i relevantnost njezinih zadaća.* Ocjenjivanjem bi trebalo procijeniti i učinak, djelotvornost i učinkovitost europskog okvira za kibersigurnosno certificiranje.

Amandman 29

Prijedlog uredbe Članak 2. – stavak 1. – točka 11.

Tekst koji je predložila Komisija

(11) „IKT proizvod ili usluga” znači *bilo koji* element ili *skupina elemenata* mrežnih i informacijskih sustava;

Izmjena

(11) „IKT *postupak*, proizvod ili usluga” znači *proizvod, usluga, postupak, sustav* ili *kombinacija navedenog koji je* element mrežnih i informacijskih sustava;

(Ova izmjena primjenjuje se u cijelom zakonodavnom tekstu koji se razmatra. Ako bude prihvaćena, bit će potrebno unijeti tehničke promjene u cijelom tekstu.)

Amandman 30

Prijedlog uredbe Članak 2. – stavak 1. – točka 11.a (nova)

Tekst koji je predložila Komisija

Izmjena

(11 a) „nacionalno tijelo za nadzor certifikacije” znači tijelo države članice

koje je odgovorno za izvršavanje zadaća praćenja, provedbe i nadzora kibersigurnosne certifikacije na svome državnom području;

Amandman 31

Prijedlog uredbe

Članak 2. – stavak 1. – točka 16.a (nova)

Tekst koji je predložila Komisija

Izmjena

(16 a) „vlastita izjava o sukladnosti” znači izjava proizvođača izjavljuje da je njegov IKT postupak, proizvod ili usluga sukladna sa specificiranim europskim programima kibersigurnosne certifikacije.

Amandman 32

Prijedlog uredbe

Članak 3. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

1. Agencija obavlja zadaće koje su joj dodijeljene ovom Uredbom kako bi pridonijela **ostvarivanju** visoke razine kibersigurnosti u Uniji.

1. Agencija obavlja zadaće koje su joj dodijeljene ovom Uredbom kako bi pridonijela **postizanju** visoke **zajedničke** razine kibersigurnosti u Uniji **radi sprečavanja kibernapada u Uniji, smanjenja rascjepkanosti na unutarnjem tržištu i poboljšanja njegova funkcioniranja.**

Amandman 33

Prijedlog uredbe

Članak 4. – stavak 5.

Tekst koji je predložila Komisija

Izmjena

5. Agencija **povećava** kibersigurnosne sposobnosti na razini Unije kako bi dopunila djelovanja država članica usmjerena na sprječavanje kiberprijetnji i odgovaranje na kiberprijetnje, posebno u

5. Agencija **pridonosi povećanju** kibersigurnosne sposobnosti na razini Unije kako bi dopunila **i jačala** djelovanja država članica usmjerena na sprječavanje kiberprijetnji i odgovaranje na

slučaju prekograničnih incidenata.

kiberprijetnje, posebno u slučaju prekograničnih incidenata.

Amandman 34

Prijedlog uredbe

Članak 4. – stavak 6.

Tekst koji je predložila Komisija

6. Agencija promiče uporabu certifikacije, među *ostalim i pridonošenjem* uspostavi i održavanju okvira za kibersigurnosnu certifikaciju na razini Unije u skladu s *glavom III. ove Uredbe* u cilju povećanja transparentnosti kibersigurnosnog jamstva IKT *proizvoda i usluga* i jačanja povjerenja u jedinstveno digitalno tržište.

Izmjena

6. Agencija promiče uporabu certifikacije, *izbjegavajući pritom rascjepkanost prouzročenu nedostatkom koordinacije* među *postojećim programima certifikacije u Uniji*. *Agencija doprinosi* uspostavi i održavanju okvira za kibersigurnosnu certifikaciju na razini Unije u skladu s *člancima 43. do 54. [glava III.]* u cilju povećanja transparentnosti kibersigurnosnog jamstva *za IKT proizvode i usluge* i jačanja povjerenja u jedinstveno digitalno tržište.

Amandman 35

Prijedlog uredbe

Članak 4. – stavak 7.

Tekst koji je predložila Komisija

7. Agencija promiče visoku razinu osviještenosti građana i poduzeća o pitanjima povezanima s kibersigurnošću.

Izmjena

7. Agencija promiče visoku razinu osviještenosti građana, *nadležnih tijela* i poduzeća o pitanjima povezanima s kibersigurnošću.

Amandman 36

Prijedlog uredbe

Članak 5. – stavak 1. – točka 1.

Tekst koji je predložila Komisija

1. pružanjem pomoći i savjeta, *osobito svojeg neovisnog mišljenja, i obavljanjem pripremih radnji* za razvoj i preispitivanje politike i prava Unije u području kibersigurnosti te sektorskih inicijativa politike i sektorskih

Izmjena

1. pružanjem pomoći i savjeta za razvoj i preispitivanje politike i prava Unije u području kibersigurnosti te sektorskih inicijativa politike i sektorskih

kibersigurnosti te sektorskih inicijativa politike i sektorskih zakonodavnih inicijativa koje uključuju pitanja povezana s kibersigurnošću;

zakonodavnih inicijativa koje uključuju pitanja povezana s kibersigurnošću;

Obrazloženje

Agencija bi trebala imati slobodu odabira instrumenata pomoći kojih će izvršavati svoje zadaće.

Amandman 37

Prijedlog uredbe

Članak 5. – stavak 1. – točka 2.a (nova)

Tekst koji je predložila Komisija

Izmjena

2a. pružanjem pomoći Europskom odboru za zaštitu podataka, osnovanom Uredbom (EU) 2016/679, pri izradi smjernica za specifikaciju tehničkih uvjeta prema kojima se voditelji obrade podataka mogu dopušteno koristiti osobnim podacima za potrebe informatičke sigurnosti u cilju zaštite svoje infrastrukture utvrđivanjem i blokiranjem napada na svoje informatičke sustave u kontekstu: (i) Uredbe (EU) 2016/679^{1a}; (ii) Direktive (EU) 2016/1148^{1b}; i (iii) Direktive 2002/58/EZ^{1c};;

^{1a} *Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).*

^{1b} *(EU) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o*

zaštititi podataka) (SL L 119, 4.5.2016., str. 1.).

^{1c} Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016, str. 1.).

Obrazloženje

Uspostava prikladnih mehanizama suradnje.

Amandman 38

Prijedlog uredbe

Članak 5. – stavak 1. – točka 4. – podtočka 2.

Tekst koji je predložila Komisija

(2) promicanja pojačane razine sigurnosti elektroničkih komunikacija, među ostalim pružanjem stručnog znanja i savjeta te olakšavanjem razmjene najbolje prakse među nadležnim tijelima;

Izmjena

(2) promicanja pojačane razine sigurnosti elektroničkih komunikacija, **pohrane podataka i obrade podataka**, među ostalim pružanjem stručnog znanja i savjeta te olakšavanjem razmjene najbolje prakse među nadležnim tijelima;

Amandman 39

Prijedlog uredbe

Članak 6. – stavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

2a. Agencija pomaže pri uspostavi i pokretanju dugoročnog europskog projekta kibersigurnosti kako bi se podupro rast neovisne industrije kibersigurnosti u EU-u te kako bi kibersigurnost postala sastavni dio cjelokupnog razvoja IKT-a u EU-u.

Obrazloženje

ENISA treba savjetovati zakonodavce pri pripremi politika kako bi EU uhvatio korak s industrijama informatičke sigurnosti u trećim zemljama. Taj bi projekt po opsegu trebao

odgovarati mjerama koje su prethodno poduzete u zrakoplovnoj industriji (primjer Airbusa). To je potrebno kako bi se razvila jača, suverena i vjerodostojna industrija informatičko-komunikacijskih tehnologija u EU-u (vidi istraživanje Odjela za znanstvena predviđanja (STOA) PE 614.531).

Amandman 40

Prijedlog uredbe

Članak 7. – stavak 5. – podstavak 1.

Tekst koji je predložila Komisija

Na zahtjev **najmanje dviju** pogođenih država članica i u isključivu svrhu pružanja savjeta za sprječavanje budućih incidenata, Agencija pruža potporu ili provodi ex-post tehničku istragu nakon obavijesti pogođenih poduzeća o incidentima koji imaju znatan učinak u skladu s Direktivom (EU) 2016/1148. Agencija provodi takvu istragu i na temelju obrazloženog zahtjeva Komisije u dogovoru s pogođenim državama članicama u slučaju incidenata koji utječu na najmanje dvije države članice.

Izmjena

Na zahtjev **jedne ili više** pogođenih država članica i u isključivu svrhu pružanja savjeta za sprječavanje budućih incidenata, Agencija pruža potporu ili provodi ex-post tehničku istragu nakon obavijesti pogođenih poduzeća o incidentima koji imaju znatan učinak u skladu s Direktivom (EU) 2016/1148. Agencija provodi takvu istragu i na temelju obrazloženog zahtjeva Komisije u dogovoru s pogođenim državama članicama u slučaju incidenata koji utječu na najmanje dvije države članice.

Amandman 41

Prijedlog uredbe

Članak 7. – stavak 8. – točka a

Tekst koji je predložila Komisija

(a) objedinjavanjem izvješća iz nacionalnih izvora kako bi se pridonijelo zajedničkoj informiranosti o stanju;

Izmjena

(a) objedinjavanjem izvješća iz nacionalnih **i međunarodnih** izvora kako bi se pridonijelo zajedničkoj informiranosti o stanju;

Amandman 42

Prijedlog uredbe

Članak 8. – stavak 1. – točka a – podtočka 1.a (nova)

Tekst koji je predložila Komisija

Izmjena

(1 a) ocjenjivanjem, u suradnji s Europskom skupinom za kibersigurnosnu certifikaciju, postupaka za izdavanje europskih kibersigurnosnih certifikata koje su uspostavila tijela za ocjenjivanje sukladnosti iz članka 51., s ciljem da se osigura da tijela za ocjenjivanje sukladnosti na isti način primjenjuju ovu Uredbu kad izdaju certifikate;

Amandman 43

Prijedlog uredbe

Članak 8. – stavak 1. – točka a – podtočka 1.b (nova)

Tekst koji je predložila Komisija

Izmjena

(1 b) provedbom neovisnih periodičnih ex post provjera sukladnosti certificiranih IKT proizvoda i usluga s europskim programima kibersigurnosne certifikacije;

Amandman 44

Prijedlog uredbe

Članak 8. – stavak 1. – točka a – podtočka 3.

Tekst koji je predložila Komisija

(3) sastavljanjem i objavljivanjem smjernica i razvojem dobre prakse u pogledu kibersigurnosnih zahtjeva za IKT proizvode i usluge, u suradnji s nacionalnim tijelima za nadzor certifikacije i industrijom;

Izmjena

*(3) sastavljanjem i objavljivanjem smjernica i razvojem dobre prakse, **među ostalim o načelima kiberhigijene i odvraćanju od tajnih „stražnjih ulaza”**, u pogledu kibersigurnosnih zahtjeva za IKT proizvode i usluge, u suradnji s nacionalnim tijelima za nadzor certifikacije i industrijom **i u okviru formalnog, standardiziranog i transparentnog postupka**;*

Amandman 45

Prijedlog uredbe

Članak 8. – stavak 1. – točka b

Tekst koji je predložila Komisija

(b) olakšavanjem uspostave i prihvaćanja europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT proizvoda i usluga te izradom, u suradnji s državama članicama, savjeta i smjernica o tehničkim područjima povezanim sa sigurnosnim zahtjevima za operatore ključnih usluga i pružatelje digitalnih usluga, te u pogledu već postojećih normi, uključujući nacionalne norme država članica, u skladu s člankom 19. stavkom 2. Direktive (EU) 2016/1148.

Izmjena

(b) *savjetovanjem s međunarodnim tijelima za normizaciju i europskim organizacijama za normizaciju o razvoju normi kako bi se osigurala prikladnost normi koje se primjenjuju u europskim programima kibersigurnosne certifikacije* i olakšavanjem uspostave i prihvaćanja **relevantnih** europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT proizvoda i usluga te izradom, u suradnji s državama članicama, savjeta i smjernica o tehničkim područjima povezanim sa sigurnosnim zahtjevima za operatore ključnih usluga i pružatelje digitalnih usluga, te u pogledu već postojećih normi, uključujući nacionalne norme država članica, u skladu s člankom 19. stavkom 2. Direktive (EU) 2016/1148;

Amandman 46

Prijedlog uredbe

Članak 8. – stavak 1. – točka ba (nova)

Tekst koji je predložila Komisija

Izmjena

(b a) sastavljanjem smjernica o načinu i vremenu kada se države članice međusobno trebaju obavijestiti kada saznaju za ranjivost koja nije javno poznata u IKT postupku, proizvodu ili usluzi koja je certificirana u skladu s glavom III. ove Uredbe, uključujući smjernice o koordinaciji politika otkrivanja ranjivosti;

Amandman 47

Prijedlog uredbe
Članak 8. – stavak 1. – točka bb (nova)

Tekst koji je predložila Komisija

Izmjena

(b b) sastavljanjem smjernica o minimalnim sigurnosnim zahtjevima za informatičke uređaje koji se prodaju u Uniji ili izvoze iz nje;

Amandman 48

Prijedlog uredbe
Članak 9. – stavak 1. – točka d

Tekst koji je predložila Komisija

Izmjena

(d) na posebnom portalu objedinjuje, organizira i stavlja na raspolaganje javnosti informacije o kibersigurnosti koje su dostavile institucije, agencije i tijela Unije;

(d) na posebnom portalu objedinjuje, organizira i stavlja na raspolaganje javnosti informacije o kibersigurnosti koje su dostavile institucije, agencije i tijela Unije, *uključujući informacije o važnim kibersigurnosnim incidentima i velikim povredama podataka*;

Amandman 49

Prijedlog uredbe
Članak 9. – stavak 1. – točka e

Tekst koji je predložila Komisija

Izmjena

(e) podiže razinu osviještenosti javnosti o rizicima povezanim s kibersigurnošću i daje smjernice o dobroj *praksi za pojedinačne korisnike* usmjerene na građane i organizacije;

(e) podiže razinu osviještenosti javnosti o rizicima povezanim s kibersigurnošću, daje smjernice o dobroj *korisničkoj praksi* usmjerene na građane i organizacije *te promiće donošenje preventivnih snažnih mjera informatičke sigurnosti i pouzdane zaštite podataka i privatnosti*;

Amandman 50

Prijedlog uredbe
Članak 9. – stavak 1. – točka ga (nova)

Tekst koji je predložila Komisija

Izmjena

(g a) podupire tješnju suradnju i razmjenu najboljih praksi među državama članicama u pogledu obrazovanja o kibersigurnosti, kiberhigijene i podizanja razine osviještenosti;

Amandman 51

Prijedlog uredbe

Članak 10. – stavak 1. – točka a

Tekst koji je predložila Komisija

(a) savjetuje Uniju i države članice o istraživačkim potrebama i prioritetima u području kibersigurnosti kako bi se omogućili učinkoviti odgovori na postojeće i nove rizike i prijetnje, među ostalim i u pogledu novih informacijskih i komunikacijskih tehnologija te onih u nastajanju, te kako bi se učinkovito upotrebljavale tehnologije za sprečavanje rizika;

Izmjena

(a) osigurava prethodno savjetovanje s relevantnim korisničkim skupinama i savjetuje Uniju i države članice o istraživačkim potrebama i prioritetima u području kibersigurnosti kako bi se omogućili učinkoviti odgovori na postojeće i nove rizike i prijetnje, među ostalim i u pogledu novih informacijskih i komunikacijskih tehnologija te onih u nastajanju, te kako bi se učinkovito upotrebljavale tehnologije za sprečavanje rizika;

Amandman 52

Prijedlog uredbe

Članak 13. – stavak 1.

Tekst koji je predložila Komisija

1. Upravljački odbor sastoji se od jednog predstavnika svake države članice i dva predstavnika **koje imenuje** Komisija. Svi predstavnici imaju pravo glasa.

Izmjena

1. Upravljački odbor sastoji se od jednog predstavnika svake države članice i dva predstavnika **koja imenuju** Komisija i **Europski parlament**. Svi predstavnici imaju pravo glasa.

Amandman 53

Prijedlog uredbe

Članak 14. – stavak 1. – točka e

Tekst koji je predložila Komisija

e) ocjenjuje i donosi konsolidirano godišnje izvješće o aktivnostima Agencije i do 1. srpnja sljedeće godine dostavlja izvješće i njegovu ocjenu Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu. Godišnje izvješće uključuje finansijske izvještaje i u njemu se opisuje kako je **Agencija** ostvarila svoje pokazatelje uspješnosti. Godišnje se izvješće objavljuje;

Izmjena

e) ocjenjuje i donosi konsolidirano godišnje izvješće o aktivnostima Agencije i do 1. srpnja sljedeće godine dostavlja izvješće i njegovu ocjenu Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu. Godišnje izvješće uključuje finansijske izvještaje i u njemu se opisuje **učinkovitost potrošenih sredstava te ocjenjuje djelotvornost Agencije** i kako je **ona** ostvarila svoje pokazatelje uspješnosti. Godišnje se izvješće objavljuje;

Amandman 54

Prijedlog uredbe

Članak 14. – stavak 1. – točka m

Tekst koji je predložila Komisija

(m) imenuje izvršnog direktora i, po potrebi, produžuje njegov mandat ili ga razrješava dužnosti u skladu s člankom 33. ove Uredbe;

Izmjena

(m) imenuje izvršnog direktora s **pomoću postupka odabira utemeljenog na kriterijima stručnosti** i, po potrebi, produžuje njegov mandat ili ga razrješava dužnosti u skladu s člankom 33. ove Uredbe;

Amandman 55

Prijedlog uredbe

Članak 14. – stavak 1. – točka o

Tekst koji je predložila Komisija

o) donosi sve odluke o unutarnjem ustrojstvu Agencije te, prema potrebi, o njegovim izmjenama, uzimajući u obzir potrebe Agencije u pogledu aktivnosti te razumno finansijsko upravljanje;

Izmjena

o) donosi sve odluke o unutarnjem ustrojstvu Agencije te, prema potrebi, o njegovim izmjenama, uzimajući u obzir potrebe Agencije u pogledu aktivnosti **navedenih u ovoj Uredbi** te razumno finansijsko upravljanje;

Amandman 56

Prijedlog uredbe

Članak 19. – stavak 2.

Tekst koji je predložila Komisija

2. Izvršni direktor na poziv izvješćuje Europski parlament o izvršavanju svojih dužnosti. Vijeće može pozvati izvršnog direktora da ga izvijesti o izvršavanju svojih dužnosti.

Izmjena

2. Izvršni direktor na poziv *ili svake godine* izvješćuje Europski parlament o izvršavanju svojih dužnosti. Vijeće može pozvati izvršnog direktora da ga izvijesti o izvršavanju svojih dužnosti.

Amandman 57

Prijedlog uredbe

Članak 20. – stavak 1.

Tekst koji je predložila Komisija

1. Upravljački odbor, djelujući na prijedlog izvršnog direktora, osniva Stalnu interesnu skupinu sastavljenu od priznatih stručnjaka koji zastupaju relevantne interesne skupine, kao što su IKT industrija, pružatelji elektroničkih komunikacijskih mreža ili usluga dostupnih javnosti, skupine potrošača, akademski stručnjaci za *kibersigurnost* i predstavnici nadležnih tijela prijavljenih u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija] te od tijela za izvršenje zakonodavstva i tijela za nadzor zaštite podataka.

Izmjena

1. Upravljački odbor, djelujući na prijedlog izvršnog direktora, osniva Stalnu interesnu skupinu sastavljenu od priznatih stručnjaka koji zastupaju relevantne interesne skupine, kao što su IKT industrija, pružatelji elektroničkih komunikacijskih mreža ili usluga dostupnih javnosti, *a posebno europska IKT industrija i pružatelji IKT usluga, udruženja malih i srednjih poduzeća, skupine i udruge* potrošača, akademski stručnjaci *u području kibersigurnosti, europske organizacije za normizaciju kako je definirano u točki 8. članka 2. Uredbe (EU) br. 1025/2012, relevantne sektorske agencije i tijela Unije* i predstavnici nadležnih tijela prijavljenih u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija] te od tijela za izvršenje zakonodavstva i tijela za nadzor zaštite podataka.

Amandman 58

Prijedlog uredbe

Članak 20. – stavak 4.

Tekst koji je predložila Komisija

4. Mandat članova Stalne interesne skupine traje dvije i pol godine. Članovi

Izmjena

4. Mandat članova Stalne interesne skupine traje dvije i pol godine. Članovi

Upravljačkog odbora ne mogu biti članovi Stalne interesne skupine. Stručnjaci Komisije i država članica imaju pravo nazočiti sjednicama Stalne interesne skupine i sudjelovati u njezinu radu. Na sastanke Stalne interesne skupine i sudjelovanje u njezinu radu mogu se pozvati predstavnici drugih tijela koja izvršni direktor smatra relevantnima koji nisu članovi Stalne interesne skupine.

Upravljačkog odbora *i Izvršnog odbora, osim izvršnog direktora*, ne mogu biti članovi Stalne interesne skupine. Stručnjaci Komisije i država članica imaju pravo nazočiti sjednicama Stalne interesne skupine i sudjelovati u njezinu radu. Na sastanke Stalne interesne skupine i sudjelovanje u njezinu radu mogu se pozvati predstavnici drugih tijela koja izvršni direktor smatra relevantnima koji nisu članovi Stalne interesne skupine.

Amandman 59

Prijedlog uredbe Članak 20. – stavak 5.

Tekst koji je predložila Komisija

5. Stalna interesna skupina savjetuje Agenciju u vezi s obavljanjem njezinih aktivnosti. Ona posebno savjetuje izvršnog direktora u vezi s izradom prijedloga programa rada Agencije i osiguravanjem komunikacije s relevantnim interesnim skupinama o svim pitanjima koja se odnose na program rada.

Izmjena

5. Stalna interesna skupina savjetuje Agenciju u vezi s obavljanjem njezinih aktivnosti. Ona posebno savjetuje izvršnog direktora u vezi s izradom prijedloga programa rada Agencije i osiguravanjem komunikacije s relevantnim interesnim skupinama o svim pitanjima koja se odnose na program rada. *Također može predložiti Komisiji da od Agencije zatraži da izradi prijedlog europskih programa kibersigurnosne certifikacije u skladu s člankom 44., bilo na vlastitu inicijativu ili nakon podnošenja prijedloga relevantnih dionika.*

Amandman 60

Prijedlog uredbe Članak 20. – stavak 5.a (novi)

Tekst koji je predložila Komisija

Izmjena

5 a. Stalna interesna skupina savjetuje Agenciju pri izradi prijedlog europskih programa kibersigurnosne certifikacije.

Amandman 61

Prijedlog uredbe

Članak 23. – stavak 2.

Tekst koji je predložila Komisija

2. Agencija osigurava da javnost i sve zainteresirane strane dobiju odgovarajuće, objektivne, pouzdane i lako dostupne informacije, posebno u pogledu rezultata njezina rada. Agencija objavljuje i izjave o interesima dane u skladu s člankom 22.

Izmjena

2. Agencija osigurava da javnost i sve zainteresirane strane dobiju odgovarajuće, objektivne, pouzdane i lako dostupne informacije, posebno u pogledu *rasprava i* rezultata njezina rada. Agencija objavljuje i izjave o interesima dane u skladu s člankom 22.

Obrazloženje

Transparentnost treba biti provediva, uzimajući u obzir primjenu članka 24.

Amandman 62

Prijedlog uredbe

Članak 43. – stavak 1.

Tekst koji je predložila Komisija

Europskim programom kibersigurnosne certifikacije **potvrđuje** se da su IKT proizvodi i usluge koji su certificirani u skladu s tim programom usklađeni s utvrđenim zahtjevima u pogledu njihove sposobnosti da se odupru, na određenoj razini jamstva, djelovanjima kojima se nastoji ugroziti dostupnost, izvornost, cjelovitost ili povjerljivost pohranjenih ili poslanih ili obrađenih podataka ili funkcija ili usluga koje se nude tim proizvodima, **postupcima**, uslugama ili sustavima ili koje su preko njih dostupne.

Izmjena

Europski program kibersigurnosne certifikacije **uspostavlja se radi povećanja razine sigurnosti na jedinstvenom digitalnom tržištu i usvajanja usklađenog pristupa za europsku certifikaciju na razini Unije te kako bi se zajamčilo da su IKT proizvodi, usluge i sustavi otporni na kibernapade.**

Njime se potvrđuje da su IKT proizvodi i usluge koji su certificirani u skladu s tim programom usklađeni s utvrđenim **zajedničkim** zahtjevima i **značajkama** u pogledu njihove sposobnosti da se odupru, na određenoj razini jamstva, djelovanjima kojima se nastoji ugroziti dostupnost, izvornost, cjelovitost ili povjerljivost pohranjenih ili poslanih ili obrađenih podataka ili funkcija ili usluga koje se nude tim **postupcima**, proizvodima, uslugama ili sustavima ili koje su preko njih dostupne.

Amandman 63

Prijedlog uredbe Članak 43.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 43.a

Program rada

Nakon savjetovanja s Europskom skupinom za kibersigurnosnu certifikaciju i Stalnom interesnom skupinom te nakon odobrenja Komisije, ENISA uspostavlja program rada koji nudi detaljan opis zajedničkih aktivnosti koje treba poduzeti na razini Unije kako bi se osigurala dosljedna primjena ove glave te koji sadrži prioritetni popis IKT proizvoda i usluga za koje smatra da im je potreban europski program kibersigurnosne certifikacije.

Program rada utvrđuje se najkasnije [šest mjeseci nakon stupanja na snagu ove Uredbe], a novi program rada utvrđuje se svake dvije godine nakon toga. Program rada mora biti javno dostupan.

Amandman 64

Prijedlog uredbe Članak 44. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

1. Na temelju zahtjeva Komisije ENISA izrađuje prijedlog europskog programa kibersigurnosne certifikacije koji je u skladu sa zahtjevima iz članaka 45., 46. i 47. ove Uredbe. Države članice *ili* Europska skupina za kibersigurnosnu certifikaciju („Skupina“) uspostavljena u skladu s člankom 53. mogu Komisiji predložiti izradu prijedloga europskog programa kibersigurnosne certifikacije.

1. Na temelju zahtjeva Komisije ENISA izrađuje prijedlog europskog programa kibersigurnosne certifikacije koji je u skladu sa zahtjevima iz članaka 45., 46. i 47. ove Uredbe. Države članice, Europska skupina za kibersigurnosnu certifikaciju („Skupina“) uspostavljena u skladu s člankom 53. *ili Stalna interesna skupina uspostavljena u skladu s člankom 20.* mogu Komisiji predložiti izradu prijedloga europskog programa kibersigurnosne certifikacije.

Amandman 65

Prijedlog uredbe Članak 44. – stavak 2.

Tekst koji je predložila Komisija

2. Pri izradi prijedloga programa iz stavka 1. ovog članka ENISA se *savjetuje sa svim* relevantnim dionicima i blisko surađuje sa Skupinom. Skupina pruža ENISA-i pomoć i stručne savjete koji su joj potrebni u vezi s izradom prijedloga programa, među ostalim davanjem mišljenja kada je potrebno.

Izmjena

2. Pri izradi prijedloga programa iz stavka 1. ovog članka ENISA se *u okviru službenog, standardiziranog i transparentnog procesa savjetuje sa Stalnom interesnom skupinom, osobito europskim organizacijama za normizaciju, i svim ostalim* relevantnim dionicima, *uključujući organizacije potrošača*, i blisko surađuje sa Skupinom *uzimajući u obzir postojeće nacionalne i međunarodne norme. Pri izradi svakog prijedloga programa ENISA sastavlja kontrolni popis rizika i odgovarajućih kibersigurnosnih znacajki.*

Skupina pruža ENISA-i pomoć i stručne savjete koji su joj potrebni u vezi s izradom prijedloga programa, među ostalim davanjem mišljenja kada je potrebno.

Kad je to relevantno, ENISA može uspostaviti i savjetodavnu interesnu skupinu stručnjaka, koja se sastoji od članova Stalne interesne skupine i svih drugih relevantnih dionika s određenim stručnim znanjem u području predmetnog predloženog programa, kako bi pružila dodatnu pomoć i savjete.

Amandman 66

Prijedlog uredbe Članak 44. – stavak 3.

Tekst koji je predložila Komisija

3. ENISA dostavlja Komisiji prijedlog europskog programa kibersigurnosne certifikacije izrađenog u skladu sa stavkom 2. ovog članka.

Izmjena

3. ENISA dostavlja Komisiji prijedlog europskog programa kibersigurnosne certifikacije izrađenog u skladu sa stavkom 2. ovog članka, *a Komisija ocjenjuje njegovu prikladnost za*

postizanje ciljeva zahtjeva iz stavka 1.

Amandman 67

Prijedlog uredbe

Članak 44. – stavak 3.a (novi)

Tekst koji je predložila Komisija

Izmjena

3a. ENISA mora čuvati poslovnu tajnu u pogledu svih podataka prikupljenih pri obavljanju svojih zadaća u skladu s ovom Uredbom.

Amandman 68

Prijedlog uredbe

Članak 44. – stavak 4.

Tekst koji je predložila Komisija

Izmjena

4. Komisija, *na temelju prijedloga programa koji je izradila ENISA, može* donositi *provedbene* akte, u skladu s člankom 55. stavkom 1., kojima su *predviđeni europski programi* kibersigurnosne certifikacije za IKT proizvode i usluge koji ispunjavaju zahtjeve iz članaka 45., 46. i 47. ove Uredbe.

4. Komisija je *ovlaštena* donositi *delegirane* akte, u skladu s člankom 55.a, *u pogledu uspostave europskih programa* kibersigurnosne certifikacije za IKT proizvode i usluge koji ispunjavaju zahtjeve iz članaka 45., 46. i 47. ove Uredbe. *Pri donošenju tih delegiranih akata Komisija temelji programe kibersigurnosne certifikacije za IKT proizvode i usluge na svim relevantnim prijedlozima programa koje je predložila ENISA. Komisija se može savjetovati s Europskim odborom za zaštitu podataka i uzeti u obzir njegovo stajalište prije donošenja takvih delegiranih akata.*

Amandman 69

Prijedlog uredbe

Članak 44. – stavak 5.

Tekst koji je predložila Komisija

Izmjena

5. ENISA održava posebno web-

5. ENISA održava posebno web-

mjesto na kojem pruža informacije i promovira europske programe kibersigurnosne certifikacije.

mjesto na kojem pruža informacije i promovira europske programe kibersigurnosne certifikacije, *uključujući informacije o svim predloženim programima čiju je pripremu od ENISA -e zatražila Komisija.*

Amandman 70

Prijedlog uredbe

Članak 45. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

Europski program kibersigurnosne certifikacije izrađuje se tako da se njime uzimaju u obzir, *prema potrebi*, sljedeći sigurnosni ciljevi:

Izmjena

Svaki europski program kibersigurnosne certifikacije izrađuje se tako da se njime uzimaju u obzir *barem* sljedeći sigurnosni ciljevi, *u mjeri u kojoj su relevantni*:

Amandman 71

Prijedlog uredbe

Članak 45. – stavak 1. – točka g

Tekst koji je predložila Komisija

(g) osigurati da *je* softver za IKT proizvode i usluge *ažuriran* i da ne *sadržava* poznate *ranjivosti* i da *ti IKT proizvodi u usluge* raspolažu mehanizmima za sigurno ažuriranje softvera.

Izmjena

(g) osigurati da *su* softver *i hardver* za IKT proizvode i usluge *ažurirani* i da ne *sadržavaju* poznate ranjivosti; *osigurati da su osmišljeni i provedeni tako* da se *njihova podložnost ranjivostima zaista ograniči te osigurati da* raspolažu mehanizmima za sigurno ažuriranje softvera, *uključujući nadogradnje hardvera i automatsko sigurnosno ažuriranje*;

Amandman 72

Prijedlog uredbe

Članak 45. – stavak 1. – točka ga (nova)

Tekst koji je predložila Komisija

Izmjena

(g a) osigurati da se IKT proizvodi i usluge razvijaju i funkcioniraju na takav

način da je visoka razina kibersigurnosti i zaštite podataka prethodno konfigurirana u skladu s načelom „integrirane sigurnosti”.

Amandman 73

Prijedlog uredbe Članak 46. – stavak 1.

Tekst koji je predložila Komisija

1. ***Europskim*** programom kibersigurnosne certifikacije može se utvrditi jedna od sljedećih razina jamstva ili više njih: ***osnovna, znatna i/ili visoka*** za IKT proizvode i usluge certificirane u skladu s tim programom.

Izmjena

1. ***Svakim europskim*** programom kibersigurnosne certifikacije može se utvrditi jedna od sljedećih razina jamstva ***utemeljenih na riziku*** ili više njih: ***„funkcionalno sigurna”, „znatno sigurna” i/ili „vrlo sigurna”*** za IKT proizvode i usluge certificirane u skladu s tim programom.

Razine jamstva za svaki prijedlog europskog programa kibersigurnosne certifikacije utvrđuju se na temelju rizika utvrđenih u kontrolnom popisu iz članka 44. stavka 2. i na temelju dostupnosti kibersigurnosnih značajki za suzbijanje tih rizika u IKT proizvodima i uslugama na koje se program certifikacije primjenjuje.

Amandman 74

Prijedlog uredbe Članak 46. – stavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

1 a. ***U svakom programu navodi se metodologija procjene ili proces evaluacije koji treba poštovati pri izdavanju certifikata na svakoj razini jamstva, ovisno o predviđenoj uporabi i riziku povezanom s IKT proizvodima i uslugama obuhvaćenim tim programom.***

Amandman 75

Prijedlog uredbe

Članak 46. – stavak 2. – uvodni dio

Tekst koji je predložila Komisija

2. **Osnovna, znatna i visoka** razina jamstva ispunjavaju sljedeće kriterije:

Izmjena

2. „**Funkcionalno sigurna**”, „**načelno sigurna**” ili „**vrlo sigurna**” razina jamstva ispunjavaju sljedeće kriterije:

Amandman 76

Prijedlog uredbe

Članak 46. – stavak 2. – točka a

Tekst koji je predložila Komisija

(a) **osnovna** razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava **ograničeni** stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha smanjiti rizik od kiberincidenata;

Izmjena

(a) „**funkcionalno sigurna**” razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava **odgovarajući** stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT **postupka**, proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha smanjiti rizik od kiberincidenata;

Amandman 77

Prijedlog uredbe

Članak 46. – stavak 2. – točka b

Tekst koji je predložila Komisija

(b) **znatna** razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava znatan stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme

Izmjena

(b) „**znatno sigurna**” razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava znatan stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT **postupka**, proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke

i postupke, uključujući tehničke kontrole, čija je svrha znatno smanjiti rizik od kiberincidenata;

specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha znatno smanjiti rizik od kiberincidenata;

Amandman 78

Prijedlog uredbe Članak 46. – stavak 2. – točka c

Tekst koji je predložila Komisija

(c) **visoka** razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava viši stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge nego certifikatima o **znatnoj** razini jamstva i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha spriječiti kiberincidente.

Izmjena

(c) „**vrlo sigurna**” razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava viši stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT **postupka**, proizvoda ili usluge nego certifikatima o **znatno sigurnoj** razini jamstva i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha spriječiti kiberincidente. *To se posebno odnosi na proizvode i usluge namijenjene operatorima ključnih usluga, kako su definirani u članku 4. stavku 4. Direktive 2016/1148/EU.*

Amandman 79

Prijedlog uredbe Članak 47. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. **Europski** program kibersigurnosne certifikacije uključuje sljedeće elemente:

Izmjena

1. **Svaki europski** program kibersigurnosne certifikacije uključuje **barem** sljedeće elemente, **kad je to primjenjivo**:

Amandman 80

Prijedlog uredbe

Članak 47. – stavak 1. – točka a

Tekst koji je predložila Komisija

(a) predmet i opseg certifikacije, uključujući vrstu ili kategorije obuhvaćenih IKT proizvoda i usluga;

Izmjena

(a) predmet i opseg *programa* certifikacije, uključujući *sve konkretne obuhvaćene sektore te* vrstu ili kategorije obuhvaćenih IKT proizvoda i usluga;

Amandman 81

Prijedlog uredbe

Članak 47. – stavak 1. – točka b

Tekst koji je predložila Komisija

(b) iscrpnu specifikaciju kibersigurnosnih zahtjeva u odnosu na koje se određeni IKT proizvodi i uslugeo cjenjuju, *na primjer* upućivanjem na *norme Unije ili međunarodne* norme ili tehničke specifikacije;

Izmjena

(b) iscrpnu specifikaciju kibersigurnosnih zahtjeva u odnosu na koje se određeni IKT proizvodi i uslugeo cjenjuju, *osobito* upućivanjem na *međunarodne, europske ili nacionalne* norme ili tehničke specifikacije;

Amandman 82

Prijedlog uredbe

Članak 47. – stavak 1. – točka ba (nova)

Tekst koji je predložila Komisija

Izmjena

(b a) iscrpnu specifikaciju može li se odobrena certifikacija primijeniti samo na pojedinačni proizvod ili na raspon proizvoda, na primjer različite inačice ili modele iste osnovne strukture proizvoda;

Amandman 83

Prijedlog uredbe

Članak 47. – stavak 1. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(c a) naznaku je li vlastita izjava o

sukladnosti dopuštena u okviru programa te mjerodavni postupak za ocjenjivanje sukladnosti ili vlastitu izjavu o sukladnosti ili oboje;

Amandman 84

Prijedlog uredbe

Članak 47. – stavak 1. – točka cb (nova)

Tekst koji je predložila Komisija

Izmjena

(c b) zahtjeve u pogledu certifikacije definirane tako da se certifikacija može uključiti u sustavne kibersigurnosne procese proizvodača koji se provode tijekom osmišljavanja, razvoja i životnog ciklusa IKT postupka, proizvoda ili usluge, ili da se certifikacija na njima može temeljiti;

Amandman 85

Prijedlog uredbe

Članak 47. – stavak 1. – točka f

Tekst koji je predložila Komisija

Izmjena

(f) ako su programom predviđeni oznake ili znakovi, uvjete pod kojim se te oznake ili znakovi mogu upotrebljavati;

*(f) ako su programom predviđeni oznake ili znakovi, **kao što je oznaka kibersigurnosne sukladnosti EU-a koja znači da IKT postupak, proizvod ili usluga udovoljava kriterijima nekog programa**, uvjete pod kojim se te oznake ili znakovi mogu upotrebljavati;*

Amandman 86

Prijedlog uredbe

Članak 47. – stavak 1. – točka g

Tekst koji je predložila Komisija

Izmjena

(g) **ako je nadzor dio programa,** pravila za praćenje sukladnosti sa

(g) pravila za praćenje sukladnosti sa zahtjevima iz certifikata, uključujući

zahtjevima iz certifikata, uključujući mehanizme za dokazivanje trajne sukladnosti s navedenim kibersigurnosnim zahtjevima;

mehanizme za dokazivanje trajne sukladnosti s navedenim kibersigurnosnim zahtjevima, *kao što su obvezna ažuriranja, nadogradnje ili zakrpe predmetnog IKT postupka, proizvoda ili usluge, kad je to relevantno i izvedivo*;

Amandman 87

Prijedlog uredbe

Članak 47. – stavak 1. – točka h

Tekst koji je predložila Komisija

(h) uvjete za izdavanje, održavanje *i* produljenje certifikata te za proširenje ili smanjenje njegova opsega;

Izmjena

(h) uvjete za izdavanje, održavanje, produljenje *i obnavljanje* certifikata te za proširenje ili smanjenje njegova opsega;

Amandman 88

Prijedlog uredbe

Članak 47. – stavak 1. – točka i

Tekst koji je predložila Komisija

(i) pravila u vezi s posljedicama nesukladnosti certificiranih proizvoda i usluga **IKT-a** sa zahtjevima za certifikaciju;

Izmjena

(i) pravila u vezi s posljedicama nesukladnosti certificiranih **IKT** proizvoda i usluga sa zahtjevima za certifikaciju *te opće informacije o kaznama utvrđenima u članku 54. ove Uredbe*;

Amandman 89

Prijedlog uredbe

Članak 47. – stavak 1. – točka j

Tekst koji je predložila Komisija

(j) pravila o tome kako prijaviti prethodno neotkrivene kibersigurnosne ranjivosti IKT proizvoda i usluga i postupiti u slučaju njihova otkrivanja;

Izmjena

(j) pravila o tome kako prijaviti prethodno neotkrivene kibersigurnosne ranjivosti IKT proizvoda i usluga i postupiti u slučaju njihova otkrivanja, *među ostalim koordiniranim procesima otkrivanja ranjivosti*;

Amandman 90

Prijedlog uredbe

Članak 47. – stavak 1. – točka I

Tekst koji je predložila Komisija

(l) utvrđivanje nacionalnih programa kibersigurnosne certifikacije kojima je obuhvaćena ista vrsta ili iste kategorije IKT proizvoda i usluga;

Izmjena

(l) utvrđivanje nacionalnih *ili međunarodnih* programa kibersigurnosne certifikacije *ili postojećih međunarodnih sporazuma o uzajamnom priznavanju* kojima je obuhvaćena ista vrsta ili iste kategorije IKT proizvoda i usluga;

Amandman 91

Prijedlog uredbe

Članak 47. – stavak 1. – točka ma (nova)

Tekst koji je predložila Komisija

Izmjena

(m a) maksimalno razdoblje valjanosti certifikata;

Amandman 92

Prijedlog uredbe

Članak 47. – stavak 1. – točka mb (novi)

Tekst koji je predložila Komisija

Izmjena

(m b) pravila za testiranje sposobnosti odupiranja i otpornosti za „vrlo sigurnu” razinu jamstva.

Amandman 93

Prijedlog uredbe

Članak 47. – stavak 3.

Tekst koji je predložila Komisija

Izmjena

3. Ako je tako predviđeno posebnim aktom Unije, certificiranje u okviru europskog programa kibersigurnosne

3. Ako je tako predviđeno posebnim *budućim* aktom Unije, certificiranje u okviru europskog programa

certifikacije može se upotrijebiti za dokazivanje prepostavke sukladnosti sa zahtjevima tog akta.

kibersigurnosne certifikacije može se upotrijebiti za dokazivanje prepostavke sukladnosti sa zahtjevima tog akta.

Amandman 94

Prijedlog uredbe Članak 48. – stavak 2.

Tekst koji je predložila Komisija

2. **Certifikacija** je dobrovoljna, osim ako je pravom Unije predviđeno drukčije.

Izmjena

2. **Certificiranje u sklopu europskog programa kibersigurnosne certifikacije obvezno je za IKT proizvode i usluge s visokom stopom inherentnog rizika koji su konkretno namijenjeni operatorima ključnih usluga, kako su definirani u članku 4. stavku 4. Direktive 2016/1148/EU. Za sve ostale IKT proizvode i usluge certifikacija je dobrovoljna, osim ako je pravom Unije predviđeno drukčije.**

Amandman 95

Prijedlog uredbe Članak 48. – stavak 3.

Tekst koji je predložila Komisija

3. **Europski certifikat o kibersigurnosti** u skladu s ovim člankom izdaju tijela za ocjenjivanje sukladnosti iz članka 51. na temelju kriterija uključenih u europski program kibersigurnosne certifikacije donesen u skladu s člankom 44.

Izmjena

3. **Europske certifikate o kibersigurnosti** u skladu s ovim člankom izdaju tijela za ocjenjivanje sukladnosti iz članka 51. na temelju kriterija uključenih u europski program kibersigurnosne certifikacije donesen u skladu s člankom 44.

Kao alternativu certificiranju koje provode tijela za ocjenjivanje sukladnosti, proizvođači proizvoda i pružatelji usluga mogu, ako je predmetnim programom predviđena takva mogućnost, dati vlastitu izjavu o sukladnosti kojom izjavljuju da neki postupak, proizvod ili usluga udovoljava kriterijima programa certificiranja. U takvim slučajevima

proizvođač proizvoda ili pružatelj usluge na zahtjev dostavlja nacionalnom tijelu za nadzor certifikacije koje je to tražilo i ENISA-i vlastitu izjavu o sukladnosti.

Amandman 96

Prijedlog uredbe

Članak 48. – stavak 4. – uvodni dio

Tekst koji je predložila Komisija

4. Odstupajući od stavka 3. u opravdanim se slučajevima u europskom **kibersigurnosnom programu** može predviđjeti da europski certifikat o kibersigurnosti u okviru tog programa može izdati samo javno tijelo. To javno tijelo može biti:

Izmjena

4. Odstupajući od stavka 3. u opravdanim se slučajevima, *kao primjerice iz razloga nacionalne sigurnosti*, u europskom **programu kibersigurnosne certifikacije** može predviđjeti da europski certifikat o kibersigurnosti u okviru tog programa može izdati samo javno tijelo. To javno tijelo može biti:

Amandman 97

Prijedlog uredbe

Članak 48. – stavak 5.

Tekst koji je predložila Komisija

5. Pravna ili fizička osoba koja prijavi svoje IKT proizvode ili usluge za postupak certifikacije dostavlja tijelu za ocjenjivanje sukladnosti iz članka 51. sve informacije potrebne za provedbu postupka certifikacije.

Izmjena

5. Pravna ili fizička osoba koja prijavi svoje IKT proizvode ili usluge za postupak certifikacije dostavlja tijelu za ocjenjivanje sukladnosti iz članka 51. sve informacije potrebne za provedbu postupka certifikacije, *uključujući informacije o svim poznatim sigurnosnim ranjivostima*.

Amandman 98

Prijedlog uredbe

Članak 48. – stavak 6.

Tekst koji je predložila Komisija

6. Certifikati se izdaju na **najviše tri godine** i mogu se obnoviti pod istim

Izmjena

6. Certifikati se izdaju *i važeći su najviše na razdoblje utvrđeno u svakom*

uvjetima ako su i dalje ispunjeni *relevantni zahtjevi*.

programu certifikacije i mogu se obnoviti pod istim uvjetima ako su *relevantni zahtjevi tog programa, uključujući sve revidirane ili izmijenjene zahtjeve*, i dalje ispunjeni.

Amandman 99

Prijedlog uredbe Članak 48. – stavak 6.a (novi)

Tekst koji je predložila Komisija

Izmjena

6 a. Certifikati vrijede i dalje za sve nove verzije postupka, proizvoda ili usluge ako je primarni razlog za novu verziju zakrpa, popravak ili drugačije rješavanje poznatih ili potencijalnih sigurnosnih slabosti ili prijetnji.

Amandman 100

Prijedlog uredbe Članak 49. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

1. Ne dovodeći u pitanje stavak 3., nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode i usluge obuhvaćene europskim programom kibersigurnosne certifikacije prestaju proizvoditi učinke od datuma utvrđenog u *provedbenom* aktu donesenom u skladu s člankom 44. stavkom 4. Postojeći nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode i usluge koji nisu obuhvaćeni europskim programom kibersigurnosne certifikacije i dalje postoje.

1. Ne dovodeći u pitanje stavak 3., nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode i usluge obuhvaćene europskim programom kibersigurnosne certifikacije prestaju proizvoditi učinke od datuma utvrđenog u *delegiranom* aktu donesenom u skladu s člankom 44. stavkom 4.

Komisija nadzire usklađenost s ovim podstavkom kako bi se izbjeglo postojanje paralelnih programa. Postojeći nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode i usluge koji nisu obuhvaćeni europskim programom kibersigurnosne certifikacije i dalje postoje.

Amandman 101

Prijedlog uredbe

Članak 49. – stavak 3.

Tekst koji je predložila Komisija

3. Postojeći certifikati izdani u okviru nacionalnih programa kibersigurnosne certifikacije ostaju na snazi do svojeg datuma isteka.

Izmjena

3. Postojeći certifikati izdani u okviru nacionalnih programa kibersigurnosne certifikacije *koji su obuhvaćeni nekim europskim programom kibersigurnosne certifikacije* ostaju na snazi do svojeg datuma isteka.

Amandman 102

Prijedlog uredbe

Članak 50. – stavak 3.

Tekst koji je predložila Komisija

3. Svako nacionalno tijelo za nadzor certifikacije neovisno je od subjekata koje nadzire u pogledu svojeg ustrojstva, odluka o financiranju, pravne strukture i odlučivanja.

Izmjena

3. Svako nacionalno tijelo za nadzor certifikacije neovisno je od subjekata koje nadzire u pogledu svojeg ustrojstva, odluka o financiranju, pravne strukture i odlučivanja *te nije tijelo za ocjenu sukladnosti ili nacionalno akreditacijsko tijelo.*

Amandman 103

Prijedlog uredbe

Članak 50. – stavak 6. – točka a

Tekst koji je predložila Komisija

(a) prate i izvršavaju primjenu odredaba iz ove glave na nacionalnoj razini i nadziru sukladnost certifikata koje su izdala tijela za ocjenjivanje sukladnosti osnovana na njihovu državnom području sa zahtjevima iz ove glave i odgovarajućeg europskog programa kibersigurnosne certifikacije;

Izmjena

(a) prate i izvršavaju primjenu odredaba iz ove glave na nacionalnoj razini *i u skladu s pravilima koje je donijela Europska skupina za kibersigurnosnu certifikaciju na temelju točke (da) članka 53. stavka 3.* nadziru sukladnost:

i. certifikata koje su izdala tijela za ocjenjivanje sukladnosti osnovana na njihovu državnom području sa zahtjevima

*iz ove glave i odgovarajućeg europskog programa kibersigurnosne certifikacije i
ii. vlastitih izjava o sukladnosti izdanih u sklopu programa za IKT postupak, proizvod ili uslugu;*

Amandman 104

Prijedlog uredbe Članak 50. – stavak 6. – točka b

Tekst koji je predložila Komisija

(b) prate *i* nadziru aktivnosti tijela za ocjenjivanje sukladnosti za potrebe ove Uredbe, među ostalim i u pogledu obavijesti tijela za ocjenjivanje sukladnosti i povezanih zadaća iz članka 52. ove Uredbe;

Izmjena

(b) prate, nadziru *i barem svake dvije godine ocjenjuju* aktivnosti tijela za ocjenjivanje sukladnosti za potrebe ove Uredbe, među ostalim i u pogledu obavijesti tijela za ocjenjivanje sukladnosti i povezanih zadaća iz članka 52. ove Uredbe;

Amandman 105

Prijedlog uredbe Članak 50. – stavak 6. – točka c

Tekst koji je predložila Komisija

(c) obrađuju pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovu državnom području, u prikladnoj mjeri istražuju predmet pritužbe i u razumnom roku obavješćuju podnositelja pritužbe o napretku i rezultatu istrage;

Izmjena

(c) obrađuju pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovним nastanom na njihovu državnom području *ili u pogledu danih vlastitih izjava o sukladnosti*, u prikladnoj mjeri istražuju predmet pritužbe i u razumnom roku obavješćuju podnositelja pritužbe o napretku i rezultatu istrage;

Amandman 106

Prijedlog uredbe Članak 50. – stavak 6. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(c a) izvješćuju ENISA-u i Europsku skupinu za kibersigurnosnu certifikaciju o rezultatima provjera iz točke (a) i ocjenjivanja iz točke (b);

Amandman 107

Prijedlog uredbe

Članak 50. – stavak 6. – točka d

Tekst koji je predložila Komisija

(d) surađuju s drugim nacionalnim tijelima za nadzor certifikacije *ili* s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj nesukladnosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim europskim programima kibersigurnosne certifikacije;

Izmjena

(d) surađuju s drugim nacionalnim tijelima za nadzor certifikacije, *nacionalnim akreditacijskim tijelima ili* drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj nesukladnosti, *uključujući prijevarne, netočne ili lažne tvrdnje o certifikaciji*, IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim europskim programima kibersigurnosne certifikacije;

Amandman 108

Prijedlog uredbe

Članak 50. – stavak 7. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(c a) povući akreditaciju tijela za ocjenjivanje sukladnosti koja se ne pridržavaju ove Uredbe;

Amandman 109

Prijedlog uredbe

Članak 50. – stavak 7. – točka e

Tekst koji je predložila Komisija

Izmjena

(e) povući, u skladu s nacionalnim

(e) povući, u skladu s nacionalnim

pravom, certifikate koji nisu u skladu s ovom Uredbom ili europskim programom kibersigurnosne certifikacije;

pravom, certifikate koji nisu u skladu s ovom Uredbom ili europskim programom kibersigurnosne certifikacije *i o tome obavijestiti nacionalna akreditacijska tijela*;

Amandman 110

Prijedlog uredbe

Članak 50. – stavak 7. – točka fa (nova)

Tekst koji je predložila Komisija

Izmjena

(fa) ENISA-i predložiti stručnjake koji bi mogli sudjelovati u radu savjetodavne interesne skupine stručnjaka iz članka 44. stavka 2.

Amandman 111

Prijedlog uredbe

Članak 50. – stavak 8. – podstavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

Komisija stavlja na raspolaganje opći elektroničko-informacijski sustav podrške za potrebe takve razmjene.

Amandman 112

Prijedlog uredbe

Članak 50.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 50.a

Istorazinska ocjena

- 1. Nacionalna tijela za nadzor certifikacije podliježu istorazinskoj ocjeni u pogledu svih aktivnosti koje provode na temelju članka 50. ove Uredbe.*
- 2. Istorazinskom ocjenom obuhvaćeni su svi postupci koje provode*

nacionalna tijela za nadzor certifikacije, posebice postupci provjere sukladnosti proizvoda koji podliježu kibersigurnosnoj certifikaciji, stručnosti osoblja, ispravnosti provjera i metodologije inspekacija, kao i točnosti rezultata. U okviru istorazinske ocjene također se ocjenjuje imaju li dotična nacionalna tijela za nadzor certifikacije dovoljno resursa za ispravno obavljanje svojih dužnosti kako je određeno člankom 50. stavkom 4.

3. Istorazinsku ocjenu nacionalnog tijela za nadzor certifikacije provode dva nacionalna tijela za nadzor certifikacije iz drugih država članica i Komisija te se ona provodi barem jednom svakih pet godina. ENISA može sudjelovati u istorazinskoj ocjeni, a o svom sudjelovanju odlučuje na temelju analize procjene rizika.

4. Komisija u skladu s člankom 55.a ima ovlasti donositi delegirne akte kako bi utvrdila plan za istorazinsku ocjenu kojim se obuhvaća razdoblje od najmanje pet godina, definiraju kriteriji za sastav tima za istorazinsku ocjenu, metodologija koja se primjenjuje za istorazinsku ocjenu, raspored, učestalost i druge zadaće povezane s istorazinskom ocjenom. Pri donošenju tih delegiranih akata Komisija u obzir uzima napomene Skupine.

5. Skupina ispituje ishod istorazinske ocjene. ENISA sastavlja sažetak ishoda i objavljuje ga.

Amandman 113

Prijedlog uredbe Članak 51. – stavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

2a. Ako proizvođači izaberu „vlastitu izjavu o sukladnosti” u skladu s člankom 48. stavkom 3., tijela za ocjenjivanje sukladnosti poduzet će dodatne korake kako bi provjerila interne postupke koje je

proizvođač proveo da bi zajamčio sukladnost svojih proizvoda i/ili usluga sa zahtjevima europskog programa kibersigurnosne certifikacije.

Amandman 114

Prijedlog uredbe

Članak 53. – stavak 3. – točka da (nova)

Tekst koji je predložila Komisija

Izmjena

(d a) donijeti obvezujuća pravila kojima se utvrđuju učestalost provjera certifikata i vlastitih izjava o sukladnosti koje provode nacionalna tijela za nadzor certifikacije te kriteriji, razmjer i opseg tih provjera i donijeti zajednička pravila i standarde za izvješćivanje u skladu s člankom 50. stavkom 6.;

Amandman 115

Prijedlog uredbe

Članak 53. – stavak 3. – točka e

Tekst koji je predložila Komisija

Izmjena

(e) analizirati relevantne promjene u području kibersigurnosne certifikacije i razmjenjivati dobru praksu o programima kibersigurnosne certifikacije;

(e) analizirati relevantne promjene u području kibersigurnosne certifikacije i razmjenjivati **informacije i** dobru praksu o programima kibersigurnosne certifikacije;

Amandman 116

Prijedlog uredbe

Članak 53. – stavak 3. – točka fa (nova)

Tekst koji je predložila Komisija

Izmjena

(f a) razmjenjivati primjere dobre prakse u vezi s istragama tijela za ocjenjivanje sukladnosti, nositeljima europskog certifikata o kibersigurnosti te proizvođačima i pružateljima usluga koji

su dali vlastite izjave o sukladnosti;

Amandman 117

Prijedlog uredbe

Članak 53. – stavak 3. – točka fb (nova)

Tekst koji je predložila Komisija

Izmjena

(fb) olakšati uskladivanje europskih programa kibersigurnosne certifikacije s međunarodno priznatim normama i, po potrebi, predložiti ENISA-i područja u kojima bi trebala surađivati s relevantnim međunarodnim i europskim organizacijama za normizaciju kako bi se riješili nedostaci ili manjkavosti u međunarodno priznatim normama;

Amandman 118

Prijedlog uredbe

Članak 53. – stavak 3. – točka fc (nova)

Tekst koji je predložila Komisija

Izmjena

(fc) pri uspostavi programa rada iz članka 43.a davati savjete ENISA-i o prioritetnom popisu IKT proizvoda i usluga za koje smatra da je potreban europski program kibersigurnosne certifikacije;

Amandman 119

Prijedlog uredbe

Članak 53. – stavak 4. – podstavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

ENISA se mora pobrinuti da dnevni red, zapisnici i evidencija donesenih odluka budu registrirani te da objavljene verzije tih dokumenata budu dostupne javnosti na internetskoj stranici ENISA-e nakon svakog sastanka Skupine.

Amandman 120

Prijedlog uredbe Članak 55.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 55.a

Izvršavanje delegiranja ovlasti

Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

Ovlast za donošenje delegiranih akata iz članka 44. stavka 4. i članka 50.a stavka 4. dodjeljuje se Komisiji na razdoblje od 5 godina počevši od [datum stupanja na snagu temeljnog zakonodavnog akta]. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 44. stavka 4. i članka 50.a stavka 4. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Meduinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

Čim doneše delegirani akt, Komisija ga istodobno priopćuje Europskom

parlamentu i Vijeću.

*Delegirani akt donesen na temelju članka
44. stavka 4. ili članka 50.a stavka 4.
stupa na snagu samo ako Europski
parlament ili Vijeće u roku od [dva
mjeseca] od priopćenja tog akta
Europskom parlamentu i Vijeću na njega
ne podnesu nikakav prigovor ili ako su
prije isteka tog roka i Europski parlament
i Vijeće obavijestili Komisiju da neće
podnijeti prigovore. Taj se rok produžuje
za [dva mjeseca] na inicijativu Europskog
parlamenta ili Vijeća.*

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Uredba o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti“)	
Referentni dokumenti	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)	
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 23.10.2017	
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	IMCO 23.10.2017	
Pridruženi odbori - datum objave na plenarnoj sjednici	18.1.2018	
Izvjestitelj(ica) za mišljenje Datum imenovanja	Nicola Danti 25.9.2017	
Razmatranje u odboru	21.2.2018	21.3.2018
Datum usvajanja	17.5.2018	
Rezultat konačnog glasovanja	+: 31 -: 2 0: 1	
Zastupnici nazočni na konačnom glasovanju	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Turcanu, Anneleen Van Bossuyt, Marco Zullo	
Zamjenici nazočni na konačnom glasovanju	Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal	
Zamjenici nazočni na konačnom glasovanju prema čl. 200. st. 2.	Inés Ayala Sender, Flavio Zanonato	

**KONAČNO GLASOVANJE POIMENIČNIM GLASOVANJEM U ODBORU KOJI
DAJE MIŠLJENJE**

31	+
ALDE	Dita Charanzová, Kaja Kallas, Jasenko Selimovic
ECR	Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
GUE/NGL	Dennis de Jong
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij
S&D	Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlène Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato
Verts/ALE	Jan Philipp Albrecht, Pascal Durand

2	-
EFDD	John Stuart Agnew, Robert Jarosław Iwaszkiewicz

1	0
ENF	Mylène Troszczynski

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani