PREDLOGI SPREMEMB 001-257
vlagatelj: Odbor za industrijo, raziskave in energetiko

Poročilo
Angelika Niebler **A8-0264/2018**
Uredba EU o kibernetski varnosti

Predlog uredbe (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Predlog spremembe 1

Predlog uredbe
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Omrežja in informacijski sistemi ter telekomunikacijska omrežja in storitve imajo ključno vlogo v družbi ter so postali temelj gospodarske rasti. Informacijske in komunikacijske tehnologije so osnova za kompleksne sisteme, ki podpirajo družbene dejavnosti, omogočajo, da naša gospodarstva delujejo v ključnih sektorjih, kot so zdravstvo, energetika, finance in promet, ter zlasti podpirajo delovanje notranjega trga.	(1) Omrežja in informacijski sistemi ter telekomunikacijska omrežja in storitve imajo ključno vlogo v družbi ter so postali temelj gospodarske rasti. Informacijske in komunikacijske tehnologije ***(IKT)*** so osnova za kompleksne sisteme, ki podpirajo ***vsakodnevne*** družbene dejavnosti, omogočajo, da naša gospodarstva delujejo v ključnih sektorjih, kot so zdravstvo, energetika, finance in promet, ter zlasti podpirajo delovanje notranjega trga.

Predlog spremembe 2

Predlog uredbe
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Med posamezniki, podjetji in	(2) Med posamezniki, podjetji in

vladami po vsej Uniji prevladuje uporaba omrežij in informacijskih sistemov. Digitalizacija in povezljivost postajata poglavitni značilnosti vse večjega števila izdelkov in storitev, s prihodom interneta stvari (IoT) pa naj bi se v naslednjem desetletju po vsej EU začelo uporabljati na milijone, morda celo milijarde povezanih digitalnih naprav. Medtem ko je vse več naprav povezanih z internetom, v njihovo zasnovo nista zadostno vključeni varnost in odpornost, kar vodi v nezadostno kibernetsko varnost. Omejeno certificiranje zato pomeni nezadostne informacije za organizacijske in posamezne uporabnike o lastnostih izdelkov in storitev IKT glede kibernetske varnosti, kar spodkopava zaupanje v digitalne rešitve.	vladami po vsej Uniji prevladuje uporaba omrežij in informacijskih sistemov. Digitalizacija in povezljivost postajata poglavitni značilnosti vse večjega števila izdelkov in storitev, s prihodom interneta stvari (IoT) pa naj bi se v naslednjem desetletju po vsej EU začelo uporabljati na milijone, morda celo milijarde povezanih digitalnih naprav. Medtem ko je vse več naprav povezanih z internetom, v njihovo zasnovo nista zadostno vključeni varnost in odpornost, kar vodi v nezadostno kibernetsko varnost. Omejeno certificiranje zato pomeni nezadostne informacije za organizacijske in posamezne uporabnike o lastnostih izdelkov***, procesov*** in storitev IKT glede kibernetske varnosti, kar spodkopava zaupanje v digitalne rešitve. ***Ta ambicija je v osrčju načrta Evropske komisije za reformo, katerega cilj je doseči enotni digitalni trg, saj omrežja informacijske in komunikacijske tehnologije zagotavljajo močno oporo digitalnim izdelkom in storitvam, ki potencialno lahko podprejo vse vidike našega življenja in poganjajo evropsko gospodarsko rast. Vzpostavljeni morajo biti bistveni tehnološki temeljniki, na katerih slonijo pomembna področja, kot so e-zdravje, internet stvari, umetna inteligenca, kvantna tehnologija, inteligentni prometni sistem in napredna proizvodnja, da bi lahko v celoti dosegli vse cilje enotnega digitalnega trga.***

Predlog spremembe 3

Predlog uredbe
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Večja digitalizacija in povezljivost vodita v večja tveganja na področju kibernetske varnosti, zaradi česar je družba na splošno bolj ranljiva za kibernetske grožnje, nevarnosti, s katerimi se srečujejo posamezniki, vključno z ranljivimi osebami, kot so otroci, pa so večje. Da bi	(3) Večja digitalizacija in povezljivost vodita v večja tveganja na področju kibernetske varnosti, zaradi česar je družba na splošno bolj ranljiva za kibernetske grožnje, nevarnosti, s katerimi se srečujejo posamezniki, vključno z ranljivimi osebami, kot so otroci, pa so večje. Da bi

ublažili tovrstno tveganje za družbo, je treba sprejeti vse potrebne ukrepe, da bi izboljšali kibernetsko varnost v EU in tako omrežja in informacijske sisteme, telekomunikacijska omrežja ter digitalne izdelke, storitve in naprave, ki jih uporabljajo posamezniki, vlade in podjetja (od malih in srednjih podjetij do upravljavcev kritičnih infrastruktur), bolje zaščitili pred kibernetskimi grožnjami.	ublažili tovrstno tveganje za družbo, je treba sprejeti vse potrebne ukrepe, da bi izboljšali kibernetsko varnost v EU in tako omrežja in informacijske sisteme, telekomunikacijska omrežja ter digitalne izdelke, storitve in naprave, ki jih uporabljajo posamezniki, vlade in podjetja (od malih in srednjih podjetij do upravljavcev kritičnih infrastruktur), bolje zaščitili pred kibernetskimi grožnjami. ***V zvezi s tem je akcijski načrt za digitalno izobraževanje, ki ga je 17. januarja 2018 objavila Evropska komisija, korak v pravo smer, zlasti z vseevropsko kampanjo ozaveščanja, namenjeno delavcem v izobraževanju, staršem in učencem, da se spodbudijo spletna varnost, kibernetska higiena in medijska pismenost ter usposabljanje za kibernetsko varnost na podlagi okvira za digitalne kompetence za državljane in da se ljudem omogoči, da uporabljajo tehnologijo z zaupanjem in odgovornostjo.***

Predlog spremembe 4

Predlog uredbe
Uvodna izjava 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Meni, da bi bilo treba cilje in naloge agencije ENISA še bolj uskladiti s skupnim sporočilom glede spodbujanje kibernetske higiene in ozaveščenosti; ugotavlja, da je kibernetsko odpornost mogoče doseči z izvajanjem temeljnih načel kibernetske higiene;

Predlog spremembe 5

Predlog uredbe
Uvodna izjava 3 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3b) Agencija ENISA bi morala za sektor kibernetske varnosti Unije zagotoviti več

praktične podpore na podlagi informacij, zlasti za MSP in zagonska podjetja, ki so ključni viri inovativnih rešitev na področju kibernetske obrambe, ter spodbujati tesnejše sodelovanje z univerzitetnimi raziskovalnimi organizacijami in pomembnimi akterji za zmanjšanje odvisnosti proizvodov kibernetske varnosti od zunanjih virov in oblikovanje strateške oskrbovalne verige znotraj Unije.

Predlog spremembe 6

Predlog uredbe
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Kibernetski napadi so vse pogostejši ter povezana gospodarstvo in družba, ki sta bolj ranljiva za kibernetske grožnje in napade, potrebujeta boljšo obrambo. Čeprav so kibernetski napadi pogosto čezmejni, so odzivi politike organov za kibernetsko varnost in pristojnosti za kazenski pregon večinoma nacionalni. Veliki kibernetski incidenti lahko povzročijo motnje pri zagotavljanju bistvenih storitev po vsej EU. Zato sta potrebna učinkovit odziv in krizno upravljanje na ravni EU, in sicer na podlagi namenskih politik in širših instrumentov za evropsko solidarnost in medsebojno pomoč. Poleg tega je za oblikovalce politike, podjetja in uporabnike zato pomembno, da se na podlagi zanesljivih podatkov Unije redno ocenjuje stanje kibernetske varnosti in odpornosti v Uniji ter sistematično napovedujejo prihodnji razvoj, izzivi in grožnje, tako na ravni Unije kot na svetovni ravni.	(4) Kibernetski napadi so vse pogostejši ter povezana gospodarstvo in družba, ki sta bolj ranljiva za kibernetske grožnje in napade, potrebujeta boljšo ***in varnejšo*** obrambo. Čeprav so kibernetski napadi pogosto čezmejni, so odzivi politike organov za kibernetsko varnost in pristojnosti za kazenski pregon večinoma nacionalni. Veliki kibernetski incidenti lahko povzročijo motnje pri zagotavljanju bistvenih storitev po vsej EU. Zato sta potrebna učinkovit odziv in krizno upravljanje na ravni EU, in sicer na podlagi namenskih politik in širših instrumentov za evropsko solidarnost in medsebojno pomoč***. Potrebe po usposabljanju na področju kibernetske obrambe so precejšnje in se še povečujejo ter se najučinkoviteje zadovoljujejo na ravni Unije.*** Poleg tega je za oblikovalce politike, podjetja in uporabnike zato pomembno, da se na podlagi zanesljivih podatkov Unije redno ocenjuje stanje kibernetske varnosti in odpornosti v Uniji ter sistematično napovedujejo prihodnji razvoj, izzivi in grožnje, tako na ravni Unije kot na svetovni ravni.

Predlog spremembe 7

Predlog uredbe
Uvodna izjava 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(5) Glede na večje izzive na področju kibernetske varnosti, s katerimi se spopada Unija, je potreben celovit sklop ukrepov, ki bi temeljili na prejšnjih ukrepih Unije in spodbujali cilje, ki se vzajemno krepijo. Ti vključujejo potrebo po nadaljnji krepitvi zmogljivosti in pripravljenosti držav članic in podjetij ter po boljšem sodelovanju in usklajevanju med državami članicami ter institucijami, agencijami in organi EU. Poleg tega je treba glede na to, da kibernetske grožnje ne poznajo meja, povečati zmogljivosti na ravni Unije, ki bi lahko dopolnjevale ukrepe držav članic, zlasti v primeru velikih čezmejnih kibernetskih incidentov in kriz. Potrebna so dodatna prizadevanja za večjo ozaveščenost državljanov in podjetij o vprašanjih kibernetske varnosti. ***Poleg tega bi bilo treba*** zaupanje v enotni digitalni trg dodatno okrepiti z zagotavljanjem preglednih informacij o ravni varnosti izdelkov in storitev IKT. To je mogoče lažje doseči s certificiranjem na ravni EU, ki bi zagotavljalo skupne zahteve in merila za ocenjevanje glede kibernetske varnosti za vse nacionalne trge in sektorje.	(5) Glede na večje izzive na področju kibernetske varnosti, s katerimi se spopada Unija, je potreben celovit sklop ukrepov, ki bi temeljili na prejšnjih ukrepih Unije in spodbujali cilje, ki se vzajemno krepijo. Ti vključujejo potrebo po nadaljnji krepitvi zmogljivosti in pripravljenosti držav članic in podjetij ter po boljšem sodelovanju in usklajevanju ***ter izmenjavi informacij*** med državami članicami ter institucijami, agencijami in organi EU. Poleg tega je treba glede na to, da kibernetske grožnje ne poznajo meja, povečati zmogljivosti na ravni Unije, ki bi lahko dopolnjevale ukrepe držav članic, zlasti v primeru velikih čezmejnih kibernetskih incidentov in kriz***, hkrati pa poudariti pomen ohranjanja in nadaljnjega izboljševanja nacionalnih zmogljivosti za odzivanje na kibernetske grožnje vseh razsežnosti***. Potrebna so dodatna prizadevanja za ***usklajen odziv EU in*** večjo ozaveščenost državljanov in podjetij o vprašanjih kibernetske varnosti. ***Glede na to, da kibernetski incidenti zmanjšujejo*** zaupanje v ***ponudnike digitalnih storitev in sam*** enotni digitalni trg***, zlasti med potrošniki, bi ga bilo treba poleg tega*** dodatno okrepiti z zagotavljanjem preglednih informacij o ravni varnosti izdelkov***, procesov*** in storitev IKT***, pri tem pa poudariti, da tudi visoka raven kibernetske varnosti ne more zagotoviti, da je izdelek ali storitev IKT povsem varen***. To je mogoče lažje doseči s certificiranjem na ravni EU, ki bi zagotavljalo skupne zahteve in merila za ocenjevanje glede kibernetske varnosti za vse nacionalne trge in sektorje***, pa tudi s spodbujanjem kibernetske pismenosti. Poleg certificiranja na ravni Unije in glede na vse večjo razpoložljivost naprav interneta stvari obstaja tudi vrsta prostovoljnih ukrepov, ki bi jih zasebni***

sektor lahko sprejel, da bi okrepil zaupanje v varnost izdelkov, procesov in storitev IKT, kot so tehnologije šifriranja in blokovne verige. Izzivi bi se morali sorazmerno odražati v proračunu, dodeljenem Agenciji, da bi se v obstoječih razmerah zagotovila optimalna funkcionalnost.

Predlog spremembe 8

Predlog uredbe
Uvodna izjava 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(5a) Za krepitev struktur evropske varnosti in kibernetske obrambe je pomembno ohranjati in razvijati zmogljivosti držav članic za celovito odzivanje na kibernetske grožnje, vključno s čezmejnimi incidenti, usklajevanje na ravni EU s strani Agencije pa ne bi smelo zmanjšati zmogljivosti ali prizadevanj v državah članicah.

Predlog spremembe 9

Predlog uredbe
Uvodna izjava 5 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(5b) Podjetja in posamezni potrošniki bi morali imeti točne informacije o stopnji varnosti svojih izdelkov IKT. Hkrati je treba razumeti, da noben izdelek ni kibernetski varen in da je treba osnovna pravila za kibernetsko higieno spodbujati in jih prednostno obravnavati.

Predlog spremembe 10

Predlog uredbe
Uvodna izjava 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) Unija je že sprejela pomembne ukrepe za zagotovitev kibernetske varnosti in okrepitev zaupanja v digitalne tehnologije. Leta 2013 je bila sprejeta strategija Evropske unije za kibernetsko varnost, ki naj bi Uniji zagotavljala smernice pri oblikovanju politike glede odziva na kibernetske grožnje in tveganja. V prizadevanjih za boljšo zaščito evropskih državljanov na spletu je Unija leta 2016 sprejela prvi zakonodajni akt na področju kibernetske varnosti, in sicer Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: direktiva o varnost omrežij in informacij). Direktiva o varnosti omrežij in informacij ***določa*** zahteve glede nacionalnih zmogljivosti na področju kibernetske varnosti, vzpostavlja prve mehanizme za okrepitev strateškega in operativnega sodelovanja med državami članicami ter uvaja obveznosti glede varnostnih ukrepov in priglasitev incidentov v vseh sektorjih, ki so ključni za gospodarstvo in družbo, npr. v energetiki, prometu, vodnem sektorju, bančništvu, infrastrukturah finančnih trgov, zdravstvu, digitalni infrastrukturi, in pri ponudnikih ključnih digitalnih storitev (iskalniki, storitve računalništva v oblaku in spletne tržnice). Pri podpori izvajanju navedene direktive je bila ključna vloga dodeljena agenciji ENISA. Poleg tega je učinkovit boj proti kibernetski kriminaliteti pomembna prednostna naloga v evropski agendi za varnost, saj prispeva k skupnemu cilju doseganja visoke ravni kibernetske varnosti.	(7) Unija je že sprejela pomembne ukrepe za zagotovitev kibernetske varnosti in okrepitev zaupanja v digitalne tehnologije. Leta 2013 je bila sprejeta strategija Evropske unije za kibernetsko varnost, ki naj bi Uniji zagotavljala smernice pri oblikovanju politike glede odziva na kibernetske grožnje in tveganja. V prizadevanjih za boljšo zaščito evropskih državljanov na spletu je Unija leta 2016 sprejela prvi zakonodajni akt na področju kibernetske varnosti, in sicer Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: direktiva o varnost omrežij in informacij). Direktiva o varnosti omrežij in informacij***, katere uspeh je močno odvisen od njenega dejanskega izvajanja v državah članicah, izpolnjuje strategijo za enotni digitalni trg ter skupaj z drugimi instrumenti, kot so Direktiva o evropskem zakoniku o elektronskih komunikacijah, Uredba (EU) 2016/679 in Direktiva 2002/58/ES, vzpostavlja*** zahteve glede nacionalnih zmogljivosti na področju kibernetske varnosti, vzpostavlja prve mehanizme za okrepitev strateškega in operativnega sodelovanja med državami članicami ter uvaja obveznosti glede varnostnih ukrepov in priglasitev incidentov v vseh sektorjih, ki so ključni za gospodarstvo in družbo, npr. v energetiki, prometu, vodnem sektorju, bančništvu, infrastrukturah finančnih trgov, zdravstvu, digitalni infrastrukturi, in pri ponudnikih ključnih digitalnih storitev (iskalniki, storitve računalništva v oblaku in spletne tržnice). Pri podpori izvajanju navedene direktive je bila ključna vloga dodeljena agenciji ENISA. Poleg tega je učinkovit boj proti kibernetski kriminaliteti pomembna prednostna naloga v evropski agendi za varnost, saj prispeva k skupnemu cilju doseganja visoke ravni kibernetske varnosti.

Predlog spremembe 11

Predlog uredbe
Uvodna izjava 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(8) Znano je, da se je po sprejetju strategije EU za kibernetsko varnost leta 2013 in po zadnji reviziji mandata Agencije splošni okvir politike znatno spremenil, tudi v zvezi z bolj negotovimi in manj varnimi svetovnimi razmerami. V tem oziru in v okviru nove politike Unije za kibernetsko varnost je treba pregledati mandat agencije ENISA, da bi opredelili njeno vlogo v spremenjenem ekosistemu kibernetske varnosti in zagotovili, da učinkovito prispeva k odzivanju Unije na izzive na področju kibernetske varnosti, ki izhajajo iz teh korenito spremenjenih groženj in za katere, kot je ugotovljeno v oceni Agencije, sedanji mandat ne zadostuje.	(8) Znano je, da se je po sprejetju strategije EU za kibernetsko varnost leta 2013 in po zadnji reviziji mandata Agencije splošni okvir politike znatno spremenil, tudi v zvezi z bolj negotovimi in manj varnimi svetovnimi razmerami. V tem oziru in v okviru ***pozitivne vloge, ki jo je odigrala Agencija skozi leta na področju zbiranja strokovnega znanja, usklajevanja in izgradnje zmogljivosti, ter v okviru*** nove politike Unije za kibernetsko varnost je treba pregledati mandat agencije ENISA, da bi opredelili njeno vlogo v spremenjenem ekosistemu kibernetske varnosti in zagotovili, da učinkovito prispeva k odzivanju Unije na izzive na področju kibernetske varnosti, ki izhajajo iz teh korenito spremenjenih groženj in za katere, kot je ugotovljeno v oceni Agencije, sedanji mandat ne zadostuje.

Predlog spremembe 12

Predlog uredbe
Uvodna izjava 11

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(11) Glede na vse večje izzive na področju kibernetske varnosti, s katerimi se spopada Unija, bi bilo treba finančne in človeške vire, dodeljene Agenciji, povečati, da bi ustrezali njeni okrepljeni vlogi in nalogam kot tudi kritičnemu položaju v sistemu organizacij, ki varujejo evropski digitalni ekosistem.	(11) Glede na vse večje ***grožnje in*** izzive na področju kibernetske varnosti, s katerimi se spopada Unija, bi bilo treba finančne in človeške vire, dodeljene Agenciji, povečati, da bi ustrezali njeni okrepljeni vlogi in nalogam kot tudi kritičnemu položaju v sistemu organizacij, ki varujejo evropski digitalni ekosistem***, kar bi Agenciji omogočilo učinkovito izvajanje njenih nalog, ki ji jih nalaga ta uredba***.

Predlog spremembe 13

Predlog uredbe
Uvodna izjava 12

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(12) Agencija bi morala razviti in ohranjati visoko raven strokovnega znanja ter delovati kot referenčna točka, ki vzbuja zaupanje v enotni trg zaradi svoje neodvisnosti, kakovosti svetovanja, ki ga zagotavlja, in informacij, ki jih razširja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog. Agencija bi morala proaktivno prispevati k prizadevanjem držav članic in Unije ter obenem opravljati svoje naloge ob popolnem sodelovanju z institucijami, organi, uradi in agencijami držav članic. Poleg tega bi moralo delo Agencije temeljiti na prispevkih in sodelovanju zasebnega sektorja ter drugih zadevnih zainteresiranih strani. Sklop nalog ***bi moral določati***, ***kako*** naj Agencija doseže ***svoje cilje, ter hkrati dopuščati*** prožnost pri njenem delovanju.	(12) Agencija bi morala razviti in ohranjati visoko raven strokovnega znanja ter delovati kot referenčna točka, ki vzbuja zaupanje v enotni trg zaradi svoje neodvisnosti, kakovosti svetovanja, ki ga zagotavlja, in informacij, ki jih razširja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog. Agencija bi morala proaktivno prispevati k prizadevanjem držav članic in Unije ter obenem opravljati svoje naloge ob popolnem sodelovanju z institucijami, organi, uradi in agencijami držav članic***, pri tem pa preprečevati podvajanje dela, spodbujati sinergijo in dopolnilnost ter s tem zagotavljati usklajenost in javnofinančne prihranke***. Poleg tega bi moralo delo Agencije temeljiti na prispevkih in sodelovanju zasebnega ***in javnega*** sektorja ter drugih zadevnih zainteresiranih strani. ***Jasno bi bilo treba opredeliti jasen načrt in*** sklop nalog ***ter ciljev***, ***ki*** naj ***jih*** Agencija doseže***, hkrati pa bi bilo treba ustrezno upoštevati potrebno*** prožnost pri njenem delovanju. ***Kolikor je mogoče, je treba ohraniti najvišjo stopnjo preglednosti in razširjanja informacij.***

Predlog spremembe 14

Predlog uredbe
Uvodna izjava 12 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(12a) Vlogo Agencije bi bilo treba stalno in pravočasno pregledovati, zlasti njeno usklajevalno vlogo v odnosu do držav članic in njihovih nacionalnih organov ter možnost, da bi delovala kot točka „vse na enem mestu“ za države članice ter organe in institucije EU. Oceniti bi bilo treba vlogo Agencije pri preprečevanju razdrobljenosti notranjega trga in

	morebitni uvedbi obveznih certifikacijskih shem za kibernetsko varnost, če bi razmere v prihodnosti to zahtevale, pa tudi njeno vlogo pri ocenjevanju izdelkov iz tretjih držav, ki vstopajo na trg EU, in morebitnem uvrščanju podjetij, ki ne izpolnjujejo meril EU, na črni seznam.

Predlog spremembe 15

Predlog uredbe
Uvodna izjava 12 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(12b) Da bi lahko zagotovila ustrezno podporo operativnemu sodelovanju v državah članicah, bi morala agencija ENISA še izboljšati svoje tehnične zmogljivosti in strokovno znanje. V ta namen bi morala Agencija postopoma okrepiti svoje osebje, namenjeno tej nalogi, da bi lahko neodvisno zbirala in analizirala različne vrste najrazličnejših groženj za kibernetsko varnost in zlonamerne programske opreme, izvajala forenzične analize in pomagala državam članicam pri odzivanju na obsežne incidente. Da bi se izognili podvajanju obstoječih zmogljivosti v državah članicah, bi morala agencija ENISA izboljšati svoje strokovno znanje in zmogljivosti na podlagi virov v državah članicah, zlasti z napotitvijo nacionalnih strokovnjakov v Agencijo, oblikovanjem nabora strokovnjakov, programi izmenjave osebja, itd.. Pri izbiri osebja, odgovornega za to področje, bi morala Agencija postopoma zagotavljati, da izpolnjuje ustrezne kriterije za zagotavljanje ustrezne podpore.

Predlog spremembe 16

Predlog uredbe
Uvodna izjava 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(13) Agencija bi morala Komisiji pomagati z nasveti, mnenji in analizami v zvezi z vsemi vprašanji Unije, povezanimi z oblikovanjem, posodabljanjem in pregledovanjem politik in prava na področju kibernetske varnosti, vključno z zaščito kritične infrastrukture in kibernetsko odpornostjo. Agencija bi morala delovati kot referenčna točka za svetovanje in strokovno znanje za sektorsko politiko in zakonodajne pobude Unije pri zadevah v zvezi s kibernetsko varnostjo.	(13) Agencija bi morala Komisiji pomagati z nasveti, mnenji in analizami v zvezi z vsemi vprašanji Unije, povezanimi z oblikovanjem, posodabljanjem in pregledovanjem politik in prava na področju kibernetske varnosti, vključno z zaščito kritične infrastrukture in kibernetsko odpornostjo. Agencija bi morala delovati kot referenčna točka za svetovanje in strokovno znanje za sektorsko politiko in zakonodajne pobude Unije pri zadevah v zvezi s kibernetsko varnostjo. ***Njeno strokovno znanje bo zlasti potrebno pri pripravi večletnega delovnega programa Unije za evropske certifikacijske sheme za kibernetsko varnost. Agencija bi morala Parlament redno obveščati o novostih, analizah in pregledih na področju kibernetske varnosti in razvoju njenih nalog.***

Predlog spremembe 17

Predlog uredbe
Uvodna izjava 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) Temeljna naloga Agencije je, da spodbuja dosledno izvajanje zadevnega pravnega okvira, zlasti učinkovito izvajanje direktive o varnosti omrežij in informacij, kar je ključno za povečanje kibernetske odpornosti. Glede na hitro razvijajoče se kibernetske grožnje je jasno, da je treba države članice podpirati s celovitejšim medsektorskim pristopom h krepitvi kibernetske odpornosti.	(14) Temeljna naloga Agencije je, da spodbuja dosledno izvajanje zadevnega pravnega okvira, zlasti učinkovito izvajanje direktive o varnosti omrežij in informacij, ***Direktive o evropskem zakoniku o elektronskih komunikacijah, Uredbe (EU) 2016/679 in Direktive 2002/58/ES,*** kar je ključno za povečanje kibernetske odpornosti. Glede na hitro razvijajoče se kibernetske grožnje je jasno, da je treba države članice podpirati s celovitejšim medsektorskim pristopom h krepitvi kibernetske odpornosti.

Predlog spremembe 18

Predlog uredbe
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Agencija bi morala državam članicam ter institucijam, organom, uradom in agencijam Unije pomagati pri njihovih prizadevanjih za vzpostavljanje in krepitev zmogljivosti in pripravljenosti za preprečevanje, odkrivanje in odzivanje na težave in incidente na področju kibernetske varnosti kot tudi pri zadevah v zvezi z varnostjo omrežij in informacijskih sistemov. Agencija bi morala zlasti podpirati razvoj in krepitev nacionalnih skupin CSIRT, da bi te dosegle visoko skupno raven zrelosti v Uniji. Agencija bi morala nuditi pomoč tudi pri oblikovanju in posodabljanju strategij Unije in držav članic za varnost omrežij in informacijskih sistemov, zlasti na področju kibernetske varnosti, ter spodbujati razširjanje teh strategij in spremljati napredek pri njihovem izvajanju. ***Poleg tega*** bi morala Agencija javnim organom ***zagotavljati usposabljanje*** in gradivo ***za usposabljanje ter po potrebi*** „usposabljati izvajalce usposabljanj“, da bi državam članicam pomagala pri razvoju ***lastnih*** zmogljivosti za usposabljanje.	(15) Agencija bi morala državam članicam ter institucijam, organom, uradom in agencijam Unije pomagati pri njihovih prizadevanjih za vzpostavljanje in krepitev zmogljivosti in pripravljenosti za preprečevanje, odkrivanje in odzivanje na težave in incidente na področju kibernetske varnosti kot tudi pri zadevah v zvezi z varnostjo omrežij in informacijskih sistemov. Agencija bi morala zlasti podpirati razvoj in krepitev nacionalnih skupin CSIRT, da bi te dosegle visoko skupno raven zrelosti v Uniji. Agencija bi morala nuditi pomoč tudi pri oblikovanju in posodabljanju strategij Unije in držav članic za varnost omrežij in informacijskih sistemov, zlasti na področju kibernetske varnosti, ter spodbujati razširjanje teh strategij in spremljati napredek pri njihovem izvajanju. ***Glede na to, da so človeške napake eno od najpomembnejših tveganj za kibernetsko varnost,*** bi morala Agencija javnim organom ***nuditi tudi usposabljanja*** in ***učno*** gradivo***, v največjem možnem obsegu pa*** „usposabljati izvajalce usposabljanj“, da bi državam članicam ***in institucijam ter agencijam Unije*** pomagala pri razvoju ***njihovih*** zmogljivosti za usposabljanje. ***Agencija bi morala služiti tudi kot kontaktna točka za države članice in institucije Unije, ki bi morale imeti možnost, da jo zaprosijo za pomoč v okviru pristojnosti in vlog, ki so ji dodeljene.***

Predlog spremembe 19

Predlog uredbe
Uvodna izjava 18

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(18) Agencija bi morala zbrati in	(18) Agencija bi morala zbrati in

analizirati nacionalna poročila skupin CSIRT in skupine CERT-EU ter določiti skupna pravila, jezik in terminologijo za izmenjavo informacij. Agencija bi morala v okviru direktive o varnosti omrežij in informacij, ki je določila temelje za prostovoljno izmenjavo tehničnih informacij na operativni ravni z ustanovitvijo mreže skupin CSIRT, vključiti tudi zasebni sektor.	analizirati nacionalna poročila skupin CSIRT in skupine CERT-EU ter določiti skupna pravila, jezik in terminologijo za izmenjavo informacij. Agencija bi morala v okviru direktive o varnosti omrežij in informacij, ki je določila temelje za prostovoljno izmenjavo tehničnih informacij na operativni ravni z ustanovitvijo mreže skupin CSIRT, vključiti tudi zasebni ***in javni*** sektor.

Predlog spremembe 20

Predlog uredbe
Uvodna izjava 19

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(19) Agencija bi morala prispevati k odzivu na ravni EU v primeru velikih čezmejnih kibernetskih incidentov in kriz. Ta naloga bi morala vključevati zbiranje ustreznih informacij ter posredovanje med mrežo skupin CSIRT, tehnično skupnostjo in nosilci odločitev, pristojnimi za krizno upravljanje. Poleg tega bi Agencija lahko nudila podporo pri obravnavi incidentov s tehničnega vidika, tako da bi olajšala ustrezno tehnično izmenjavo rešitev med državami članicami in zagotavljala informacije za komuniciranje z javnostjo. Agencija bi morala ta proces podpirati s preskušanjem načinov takšnega sodelovanja v okviru vsakoletnih vaj na področju kibernetske varnosti.	(19) Agencija bi morala prispevati k odzivu na ravni EU v primeru velikih čezmejnih kibernetskih incidentov in kriz. Ta naloga bi morala vključevati ***sklic organov držav članic in pomoč pri usklajevanju njihovega odziva,*** zbiranje ustreznih informacij ter posredovanje med mrežo skupin CSIRT, tehnično skupnostjo in nosilci odločitev, pristojnimi za krizno upravljanje. Poleg tega bi Agencija lahko nudila podporo pri obravnavi incidentov s tehničnega vidika, ***na primer*** tako***,*** da bi olajšala ustrezno tehnično izmenjavo rešitev med državami članicami in zagotavljala informacije za komuniciranje z javnostjo. Agencija bi morala ta proces podpirati s preskušanjem načinov takšnega sodelovanja v okviru vsakoletnih vaj na področju kibernetske varnosti. ***Spoštovati bi morala pristojnosti držav članic na področju kibernetske varnosti, zlasti tistih, ki se nanašajo na javno varnost, obrambo in nacionalno varnost ter dejavnosti države na področju kazenskega prava.***

Predlog spremembe 21

Predlog uredbe
Uvodna izjava 25

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(25) Države članice lahko podjetja, ki jih je incident prizadel, povabijo, naj sodelujejo z zagotavljanjem potrebnih informacij in pomoči Agenciji, brez poseganja v njihovo pravico do varovanja poslovno občutljivih informacij.	(25) Države članice lahko podjetja, ki jih je incident prizadel, povabijo, naj sodelujejo z zagotavljanjem potrebnih informacij in pomoči Agenciji, brez poseganja v njihovo pravico do varovanja poslovno občutljivih informacij ***in informacij, ki so pomembne za javno varnost***.

Predlog spremembe 22

Predlog uredbe
Uvodna izjava 26

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(26) Agencija mora za boljše razumevanje izzivov na področju kibernetske varnosti in z namenom zagotavljanja dolgoročnega strateškega svetovanja državam članicam in institucijam Unije analizirati sedanja in nastajajoča tveganja. V ta namen bi morala Agencija v sodelovanju z državami članicami ter po potrebi statističnimi uradi in drugimi organi zbirati ustrezne informacije ter opravljati analize nastajajočih tehnologij in tematske ocene o pričakovanih družbenih, pravnih, gospodarskih in regulativnih vplivih tehnoloških inovacij na varnost omrežij in informacij, zlasti na kibernetsko varnost. Agencija bi morala poleg tega države članice ter institucije, agencije in organe Unije podpirati pri prepoznavanju novih trendov in preprečevanju težav v zvezi s kibernetsko varnostjo z opravljanjem analiz groženj in ***incidentov***.	(26) Agencija mora za boljše razumevanje izzivov na področju kibernetske varnosti in z namenom zagotavljanja dolgoročnega strateškega svetovanja državam članicam in institucijam Unije analizirati sedanja in nastajajoča tveganja***, incidente, grožnje in šibke točke***. V ta namen bi morala Agencija v sodelovanju z državami članicami ter po potrebi statističnimi uradi in drugimi organi zbirati ustrezne informacije ter opravljati analize nastajajočih tehnologij in tematske ocene o pričakovanih družbenih, pravnih, gospodarskih in regulativnih vplivih tehnoloških inovacij na varnost omrežij in informacij, zlasti na kibernetsko varnost. Agencija bi morala poleg tega države članice ter institucije, agencije in organe Unije podpirati pri prepoznavanju novih trendov in preprečevanju težav v zvezi s kibernetsko varnostjo z opravljanjem analiz groženj***, incidentov*** in ***šibkih točk***.

Predlog spremembe 23

Predlog uredbe
Uvodna izjava 27

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(27) Da bi povečali odpornost Unije, bi morala Agencija razvijati odličnost na področju varnosti internetne infrastrukture in kritičnih infrastruktur z zagotavljanjem svetovanja, smernic in najboljših praks. Agencija bi morala z namenom zagotavljanja lažjega dostopa do bolje strukturiranih informacij o kibernetskih tveganjih in možnih rešitvah razvijati in vzdrževati „informacijsko vozlišče“ Unije – portal „vse na enem mestu“, ki bi javnosti nudil informacije o kibernetski varnosti, ki izhajajo iz institucij, agencij in organov EU in držav članic.	(27) Da bi povečali odpornost Unije, bi morala Agencija razvijati odličnost na področju varnosti internetne infrastrukture in kritičnih infrastruktur z zagotavljanjem svetovanja, smernic in najboljših praks. Agencija bi morala z namenom zagotavljanja lažjega dostopa do bolje strukturiranih informacij o kibernetskih tveganjih in možnih rešitvah razvijati in vzdrževati „informacijsko vozlišče“ Unije – portal „vse na enem mestu“, ki bi javnosti nudil informacije o kibernetski varnosti, ki izhajajo iz institucij, agencij in organov EU in držav članic. ***Lažji dostop do bolje strukturiranih informacij o tveganjih kibernetske varnosti in možnih rešitvah bi moral državam članicam pomagati pri izboljšanju svojih zmogljivosti in usklajevanju svojih praks, s čimer bi se povečala njihova splošna odpornost na kibernetske napade.***

Predlog spremembe 24

Predlog uredbe
Uvodna izjava 28

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(28) Agencija bi morala prispevati k ozaveščanju javnosti o tveganjih glede kibernetske varnosti in zagotavljati smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom in ***organizacijam***. Agencija bi morala prispevati tudi k spodbujanju najboljših praks in rešitev na ravni posameznikov in ***organizacij*** z zbiranjem in analiziranjem javno dostopnih informacij o pomembnih incidentih ter pripravljanjem poročil***,*** da bi zagotovila smernice za podjetja in državljane ter izboljšala splošno raven pripravljenosti in odpornosti. Agencija bi morala poleg tega v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizirati redne kampanje ozaveščanja in	(28) Agencija bi morala prispevati k ozaveščanju javnosti o tveganjih glede kibernetske varnosti***, vključno s spodbujanjem izobraževanja,*** in zagotavljati smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom***, organizacijam*** in ***podjetjem***. Agencija bi morala prispevati tudi k spodbujanju najboljših praks ***na področju kibernetske higiene, kar zajema različne prakse, ki bi jih bilo treba redno izvajati, da bi zaščitili uporabnike in podjetja na spletu,*** in rešitev na ravni posameznikov***,*** ***organizacij*** in ***podjetij*** z zbiranjem in analiziranjem javno dostopnih informacij o pomembnih incidentih ter pripravljanjem ***in objavljanjem*** poročil ***ter priročnikov*** da bi zagotovila smernice za podjetja in

redne javne izobraževalne kampanje za končne uporabnike, katerih namen je spodbujati varnejše ravnanje posameznikov na spletu in povečati ozaveščenost o potencialnih grožnjah v kibernetskem prostoru, vključno s kibernetsko kriminaliteto, kot so napadi z zvabljanjem, botneti, finančne in bančne goljufije, pa tudi spodbujati osnovno svetovanje o avtentikaciji in varstvu podatkov. Agencija bi morala imeti osrednjo vlogo pri pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav.

državljane ter izboljšala splošno raven pripravljenosti in odpornosti. ***Agencija ENISA bi si morala prizadevati tudi za to, da bi potrošnikom zagotovila ustrezne informacije o veljavnih certifikacijskih shemah, na primer z zagotavljanjem smernic in priporočil za spletne in nespletne trge. Agencija*** bi morala poleg tega v ***skladu z akcijskim načrtom za digitalno izobraževanje v*** sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizirati redne kampanje ozaveščanja in redne javne izobraževalne kampanje za končne uporabnike, katerih namen je spodbujati varnejše ravnanje posameznikov na spletu***, digitalno pismenost*** in povečati ozaveščenost o potencialnih grožnjah v kibernetskem prostoru, vključno s kibernetsko kriminaliteto, kot so napadi z zvabljanjem, botneti, finančne in bančne goljufije, pa tudi spodbujati osnovno svetovanje o ***večstopenjski*** avtentikaciji***, nameščanju popravkov, šifriranju, anonimizaciji*** in varstvu podatkov. Agencija bi morala imeti osrednjo vlogo pri pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav ***in varni uporabi storitev ter spodbujanju uporabe vgrajene varnosti, vgrajene zasebnosti in rešitev za incidente na ravni EU. Pri doseganju tega cilja mora Agencija čim bolje izkoristiti razpoložljive primere najboljše prakse in izkušnje, zlasti akademske institucije in raziskovalce na področju varnosti IT. Glede na to, da so človeške napake in nepoznavanje tveganj kibernetske varnosti glavni dejavnik negotovosti pri kibernetski varnosti, bi bilo treba Agenciji zagotoviti ustrezne vire za izvajanje te funkcije v največjem možnem obsegu.***

Predlog spremembe 25

Predlog uredbe
Uvodna izjava 28 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(28a) Agencija bi morala povečati ozaveščenost javnosti o nevarnostih goljufije s podatki in kraje podatkov, ki lahko hudo ogrozijo temeljne pravice posameznikov in pravno državo ter omajejo stabilnost demokratičnih družb ter demokratične procese v državah članicah.

Predlog spremembe 26

Predlog uredbe
Uvodna izjava 30

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(30) Da bi ***zagotovili, da*** lahko Agencija v celoti ***izpolni*** svoje cilje, bi morala sodelovati z ustreznimi institucijami, agencijami in organi, vključno s skupino CERT-EU, Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) pri Europolu, Evropsko obrambno agencijo (EDA), Evropsko agencijo za operativno upravljanje obsežnih informacijskih sistemov (eu-LISA), Evropsko agencijo za varnost v letalstvu (EASA) in vsemi drugimi agencijami EU, ki se ukvarjajo s kibernetsko varnostjo. Prav tako bi morala sodelovati z organi, ki se ukvarjajo z varstvom podatkov, da bi izmenjevala tehnično znanje in izkušnje ter najboljše prakse kot tudi nudila svetovanje glede vidikov kibernetske varnosti, ki bi lahko vplivali na njihovo delo. Predstavniki organov odkrivanja in pregona ter organov za varstvo podatkov na ravni držav članic in na ravni Unije bi morali imeti možnost, da so zastopani v ***stalni*** skupini ***zainteresiranih strani*** Agencije. Agencija bi morala pri sodelovanju z organi odkrivanja in pregona v zvezi z vidiki varnosti omrežij in informacij, ki bi lahko vplivali na njihovo delo, upoštevati obstoječe informacijske poti in vzpostavljena omrežja.	(30) Da bi lahko Agencija v celoti ***izpolnila*** svoje cilje, bi morala sodelovati z ustreznimi institucijami***, nadzornimi in drugimi pristojnimi organi EU***, agencijami in organi, vključno s skupino CERT-EU, Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) pri Europolu, Evropsko obrambno agencijo (EDA), ***Agencijo za evropski GNSS (GSA), Organ evropskih regulatorjev za elektronske komunikacije (BEREC),*** Evropsko agencijo za operativno upravljanje obsežnih informacijskih sistemov (eu-LISA), Evropsko ***centralno banko (ECB), Evropskim bančnim organom (EBA), Evropskim odborom za varstvo podatkov, Evropsko*** agencijo za varnost v letalstvu (EASA)***,*** in vsemi drugimi agencijami EU, ki se ukvarjajo s kibernetsko varnostjo. Prav tako bi morala sodelovati z ***evropskimi organizacijami za standardizacijo, ustreznimi zainteresiranimi stranmi in*** organi, ki se ukvarjajo z varstvom podatkov, da bi izmenjevala tehnično znanje in izkušnje ter najboljše prakse kot tudi nudila svetovanje glede vidikov kibernetske varnosti, ki bi lahko vplivali na njihovo delo. Predstavniki organov odkrivanja in pregona ter organov za varstvo podatkov na ravni držav članic in na ravni Unije bi

	morali imeti možnost, da so zastopani v ***svetovalni*** skupini agencije ***ENISA***. Agencija bi morala pri sodelovanju z organi odkrivanja in pregona v zvezi z vidiki varnosti omrežij in informacij, ki bi lahko vplivali na njihovo delo, upoštevati obstoječe informacijske poti in vzpostavljena omrežja. ***Vzpostaviti bi morala partnerstva z akademskimi ustanovami, ki imajo raziskovalne pobude na ustreznih področjih, ter ustrezne kanale za prispevke potrošniških in drugih organizacij, ki bi jih morala vedno preučiti.***

Predlog spremembe 27

Predlog uredbe
Uvodna izjava 31

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(31) Agencija bi morala kot članica, ki poleg tega zagotavlja sekretariat za mrežo skupin CSIRT, podpirati skupine CSIRT držav članic in skupino CERT-EU pri operativnem sodelovanju pri vseh zadevnih nalogah mreže skupin CSIRT, kot so opredeljene v direktivi o varnosti omrežij in informacij. Nadalje bi morala Agencija spodbujati in podpirati sodelovanje med ustreznimi skupinami CSIRT v primeru incidentov, napadov ali motenj omrežij ali infrastrukture, ki jo upravljajo ali varujejo skupine CSIRT, in ki vključujejo ali bi lahko vključevali najmanj dve skupini CERT, ob upoštevanju standardnih operativnih postopkov mreže skupin CSIRT.	(31) Agencija bi morala kot članica, ki poleg tega zagotavlja sekretariat za mrežo skupin CSIRT, podpirati skupine CSIRT držav članic in skupino CERT-EU pri operativnem sodelovanju pri vseh zadevnih nalogah mreže skupin CSIRT, kot so opredeljene v direktivi o varnosti omrežij in informacij. Nadalje bi morala Agencija spodbujati in podpirati sodelovanje med ustreznimi skupinami CSIRT v primeru incidentov, napadov ali motenj omrežij ali infrastrukture, ki jo upravljajo ali varujejo skupine CSIRT, in ki vključujejo ali bi lahko vključevali najmanj dve skupini CERT, ob upoštevanju standardnih operativnih postopkov mreže skupin CSIRT. ***Agencija lahko na zahtevo Komisije ali države članice izvaja redne neodvisne revizije informacijske varnosti kritične čezmejne infrastrukture, da bi opredelila morebitna tveganja za kibernetsko varnost in pripravila priporočila za okrepitev njihove odpornosti.***

Predlog spremembe 28

Predlog uredbe
Uvodna izjava 33

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(33) Agencija bi morala še naprej razvijati in ohranjati svoje strokovno znanje na področju certificiranja kibernetske varnosti, da bi lahko podpirala politike Unije na tem področju. ***Agencija*** bi morala spodbujati uporabo certificiranja kibernetske varnosti v Uniji, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije, da bi tako okrepila preglednost zagotovil izdelkov in storitev IKT glede kibernetske varnosti kot tudi zaupanje na digitalnem notranjem trgu.	(33) Agencija bi morala še naprej razvijati in ohranjati svoje strokovno znanje na področju certificiranja kibernetske varnosti, da bi lahko podpirala politike Unije na tem področju. ***Opirati*** bi ***se*** morala ***na primere najboljše prakse in*** spodbujati uporabo certificiranja kibernetske varnosti v Uniji, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije, da bi tako okrepila preglednost zagotovil izdelkov in storitev IKT glede kibernetske varnosti kot tudi zaupanje na digitalnem notranjem trgu.

Predlog spremembe 29

Predlog uredbe
Uvodna izjava 35

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(35) Agencija bi morala države članice in ponudnike storitev spodbujati k zvišanju njihovih splošnih varnostnih standardov, da ***bi vsi uporabniki*** interneta ***lahko ustrezno poskrbeli*** za ***svojo osebno kibernetsko varnost***. Natančneje, ponudniki storitev in proizvajalci izdelkov bi morali umakniti s trga ali reciklirati izdelke in storitve, ki ne izpolnjujejo ***standardov*** kibernetske varnosti. Agencija ENISA lahko v sodelovanju s pristojnimi organi razširja informacije o ravni kibernetske varnosti izdelkov in storitev na notranjem trgu ter izdaja opozorila, namenjena ponudnikom storitev in proizvajalcem, s katerimi od njih zahteva, da izboljšajo varnost, tudi kibernetsko, svojih izdelkov in ***storitev***.	(35) Agencija bi morala države članice ***,*** ***proizvajalce*** in ponudnike storitev spodbujati k zvišanju njihovih splošnih varnostnih standardov ***za svoje izdelke***, ***postopke, storitve in sisteme IKT, ki bi morali biti skladni z osnovnimi varnostnimi obveznostmi v skladu z načelom vgrajene in privzete varnosti, zlasti z zagotavljanjem potrebnih posodobitev, tako*** da ***se lahko vse uporabnike*** interneta ***zavaruje in spodbuja k sprejetju potrebnih ukrepov*** za ***zagotovitev lastne osebne kibernetske varnosti***. Natančneje, ponudniki storitev in proizvajalci izdelkov bi morali ***odpoklicati,*** umakniti s trga ali reciklirati izdelke in storitve, ki ne izpolnjujejo ***osnovnih obveznosti glede*** kibernetske varnosti***, uvozniki in distributerji pa bi morali zagotoviti, da izdelki, procesi, storitve in***

	sistemi IKT, ki jih dajejo na trg EU, izpolnjujejo veljavne zahteve in ne pomenijo tveganja za evropske potrošnike. Agencija ENISA lahko v sodelovanju s pristojnimi organi razširja informacije o ravni kibernetske varnosti izdelkov in storitev na notranjem trgu ter izdaja opozorila, namenjena ponudnikom storitev in proizvajalcem, s katerimi od njih zahteva, da izboljšajo varnost, tudi kibernetsko, svojih izdelkov***, procesov, storitev*** in ***sistemov. Agencija bi si morala skupaj z zainteresiranimi stranmi prizadevati za vseevropski pristop k odgovornemu razkrivanju šibkih točk in spodbujati primere najboljše prakse na tem področju.***

Predlog spremembe 30

Predlog uredbe
Uvodna izjava 36

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(36) Agencija bi morala v celoti upoštevati tekoče dejavnosti na področju raziskav, razvoja in tehnološkega ocenjevanja, zlasti tiste, ki potekajo v okviru raznih raziskovalnih pobud Unije, da bi lahko svetovala institucijam, organom, uradom in agencijam Unije ter, po potrebi in na njihovo zahtevo, državam članicam glede potreb pri raziskavah na področju varnosti omrežij in informacij, zlasti kibernetske varnosti.	(36) Agencija bi morala v celoti upoštevati tekoče dejavnosti na področju raziskav, razvoja in tehnološkega ocenjevanja, zlasti tiste, ki potekajo v okviru raznih raziskovalnih pobud Unije, da bi lahko svetovala institucijam, organom, uradom in agencijam Unije ter, po potrebi in na njihovo zahtevo, državam članicam glede potreb pri raziskavah na področju varnosti omrežij in informacij, zlasti kibernetske varnosti. ***Natančneje, vzpostaviti bi bilo treba sodelovanje z Evropskim raziskovalnim svetom (ERC) in Evropski inštitutom za inovacije in tehnologijo (EIT), raziskave na področju varnosti pa bi bilo treba vključiti v deveti okvirni program za raziskave (FP9) in Obzorje 2020.***

Predlog spremembe 31

Predlog uredbe

Uvodna izjava 36 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(36a) Standardi so prostovoljno, tržno usmerjeno orodje za oblikovanje tehničnih zahtev in smernic, ki je nastalo na podlagi odprtega, preglednega in vključujočega postopka. Agencija bi se morala redno posvetovati in tesno sodelovati z evropskimi organizacijami za standardizacijo, zlasti pri pripravi evropskih certifikacijskih shem za kibernetsko varnost.

Predlog spremembe 32

Predlog uredbe
Uvodna izjava 37

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(37) Težave, povezane s kibernetsko varnostjo, imajo svetovno razsežnost. Da bi se izboljšali varnostni standardi, je potrebno tesnejše mednarodno sodelovanje, vključno z opredelitvijo skupnih pravil ***ravnanja***, izmenjavo informacij ***in spodbujanjem hitrejšega*** mednarodnega sodelovanja pri odzivanju na zadeve, ki se nanašajo na varnost omrežij in informacij, pa tudi skupnega globalnega pristopa do teh vprašanj. V ta namen bi morala Agencija podpirati nadaljnjo udeležbo in sodelovanje Unije s tretjimi državami in mednarodnimi organizacijami, tako da bi po potrebi ustreznim institucijam, organom, uradom in agencijam Unije zagotavljala potrebno strokovno znanje in analize.	(37) Težave, povezane s kibernetsko varnostjo, imajo svetovno razsežnost. Da bi se izboljšali varnostni standardi, je potrebno tesnejše mednarodno sodelovanje, vključno z opredelitvijo skupnih pravil ***obnašanja in kodeksa vedenja, uporabo mednarodnih standardov***, izmenjavo informacij***,*** ***spodbujanjem hitrejše vzpostavitve*** mednarodnega sodelovanja pri odzivanju na zadeve, ki se nanašajo na varnost omrežij in informacij, pa tudi skupnega globalnega pristopa do teh vprašanj. V ta namen bi morala Agencija podpirati nadaljnjo udeležbo in sodelovanje Unije s tretjimi državami in mednarodnimi organizacijami, tako da bi po potrebi ustreznim institucijam, organom, uradom in agencijam Unije zagotavljala potrebno strokovno znanje in analize.

Predlog spremembe 33

Predlog uredbe
Uvodna izjava 40

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(40) Upravni odbor, ki ***ga sestavljajo predstavniki držav članic in Komisije***, bi moral določati splošno usmeritev dejavnosti Agencije in zagotavljati, da ta naloge opravlja v skladu s to uredbo. Na upravni odbor bi bilo treba prenesti pooblastila, potrebna za pripravo proračuna, preverjanje njegovega izvrševanja, sprejetje ustreznih finančnih pravil, uvedbo preglednih delovnih postopkov za sprejemanje odločitev Agencije, sprejetje enotnega programskega dokumenta Agencije in lastnega poslovnika, imenovanje izvršnega direktorja ter odločitev o podaljšanju in koncu mandata izvršnega direktorja.	(40) Upravni odbor, ki ***zastopa države članice in Komisijo ter zainteresirane strani, relevantne za cilje Agencije***, bi moral določati splošno usmeritev dejavnosti Agencije in zagotavljati, da ta naloge opravlja v skladu s to uredbo. Na upravni odbor bi bilo treba prenesti pooblastila, potrebna za pripravo proračuna, preverjanje njegovega izvrševanja, sprejetje ustreznih finančnih pravil, uvedbo preglednih delovnih postopkov za sprejemanje odločitev Agencije, sprejetje enotnega programskega dokumenta Agencije in lastnega poslovnika, imenovanje izvršnega direktorja ter odločitev o podaljšanju in koncu mandata izvršnega direktorja. ***Ker so naloge Agencije zelo tehnične in znanstvene, bi morali imeti člani upravnega odbora ustrezne izkušnje in visoko raven strokovnega znanja s področij delovanja Agencije.***

Predlog spremembe 34

Predlog uredbe
Uvodna izjava 41

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(41) Da bi Agencija pravilno in učinkovito delovala, bi morale Komisija in države članice zagotoviti, da imajo osebe, ki so imenovane v upravni odbor, ustrezno strokovno znanje in izkušnje na funkcijskih področjih. Komisija in države članice bi si morale prizadevati tudi za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje.	(41) Da bi Agencija pravilno in učinkovito delovala, bi morale Komisija in države članice zagotoviti, da imajo osebe, ki so imenovane v upravni odbor, ustrezno strokovno znanje in izkušnje na funkcijskih področjih. Komisija in države članice bi si morale prizadevati tudi za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje. ***Ker imajo znanja in spretnosti, potrebne za delo v Agenciji, visoko tržno vrednost, je treba zagotoviti, da so plače in socialni pogoji, ponujeni vsem zaposlenim v Agenciji, konkurenčni, da bi se za delo v njej lahko odločali najboljši strokovnjaki.***

Obrazložitev

Da bi imela agencija ENISA ustrezno raven strokovnega znanja, mora biti konkurenčen delodajalec na zelo konkurenčnem trgu.

Predlog spremembe 35

Predlog uredbe
Uvodna izjava 42

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(42) Da bi Agencija delovala nemoteno, je treba njenega izvršnega direktorja imenovati na podlagi zaslug ter dokazanih upravnih in vodstvenih sposobnosti ter ustrezne usposobljenosti in izkušenj s področja kibernetske varnosti, izvršni direktor pa mora svoje naloge opravljati popolnoma neodvisno. V ta namen bi moral izvršni direktor po predhodnem posvetovanju s Komisijo pripraviti predlog delovnega programa Agencije ter sprejeti vse potrebne ukrepe, da bi zagotovil nemoteno izvajanje delovnega programa Agencije. Izvršni direktor bi moral pripraviti letno poročilo, ki se predloži upravnemu odboru, ter osnutek poročila o načrtu prihodkov in odhodkov za Agencijo ter izvrševati proračun. Nadalje bi moral izvršni direktor imeti možnost, da ustanovi ad hoc delovne skupine, da preučijo posamezna vprašanja, zlasti znanstvene, tehnološke, pravne ali družbeno-gospodarske narave. Izvršni direktor bi moral zagotoviti, da so člani ad hoc delovnih skupin izbrani v skladu z najvišjimi strokovnimi standardi, pri čemer bi moral glede na posamezno vprašanje ustrezno upoštevati ravnovesje med predstavniki javnih uprav držav članic, institucij Unije in zasebnega sektorja, vključno s podjetji, uporabniki in znanstveniki s področja varnosti omrežij in informacij.	(42) Da bi Agencija delovala nemoteno, je treba njenega izvršnega direktorja imenovati na podlagi zaslug ter dokazanih upravnih in vodstvenih sposobnosti ter ustrezne usposobljenosti in izkušenj s področja kibernetske varnosti, izvršni direktor pa mora svoje naloge opravljati popolnoma neodvisno. V ta namen bi moral izvršni direktor po predhodnem posvetovanju s Komisijo pripraviti predlog delovnega programa Agencije ter sprejeti vse potrebne ukrepe, da bi zagotovil nemoteno izvajanje delovnega programa Agencije. Izvršni direktor bi moral pripraviti letno poročilo, ki se predloži upravnemu odboru, ter osnutek poročila o načrtu prihodkov in odhodkov za Agencijo ter izvrševati proračun. Nadalje bi moral izvršni direktor imeti možnost, da ustanovi ad hoc delovne skupine, da preučijo posamezna vprašanja, zlasti znanstvene, tehnološke, pravne ali družbeno-gospodarske narave. Izvršni direktor bi moral zagotoviti, da so člani ad hoc delovnih skupin izbrani v skladu z najvišjimi strokovnimi standardi, pri čemer bi moral glede na posamezno vprašanje ustrezno upoštevati ***uravnoteženo zastopanost spolov ter*** ravnovesje med predstavniki javnih uprav držav članic, institucij Unije in zasebnega sektorja, vključno s podjetji, uporabniki in znanstveniki s področja varnosti omrežij in informacij.

Predlog spremembe 36

Predlog uredbe
Uvodna izjava 44

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(44) Agencija bi morala imeti ***stalno*** skupino ***zainteresiranih strani***, ki bi delovala kot svetovalni organ, da bi zagotovila reden dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi zainteresiranimi stranmi. ***Stalna*** skupina ***zainteresiranih strani***, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, bi morala obravnavati zadeve, ki so pomembne za zainteresirane strani, in o njih obvestiti Agencijo. Sestava stalne skupine zainteresiranih strani, ki naj bi podala svoj prispevek predvsem glede osnutka delovnega programa, in naloge, dodeljene tej skupini, bi morale zagotoviti zadostno zastopanost zainteresiranih strani pri delu Agencije.	(44) Agencija bi morala imeti ***svetovalno*** skupino ***agencije ENISA***, ki bi delovala kot svetovalni organ, da bi zagotovila reden dialog z zasebnim sektorjem, združenji potrošnikov***, znanstveno skupnostjo*** in drugimi ustreznimi zainteresiranimi stranmi. ***Svetovalna*** skupina ***agencije ENISA***, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, bi morala obravnavati zadeve, ki so pomembne za zainteresirane strani, in o njih obvestiti Agencijo. Sestava stalne skupine zainteresiranih strani, ki naj bi podala svoj prispevek predvsem glede osnutka delovnega programa, in naloge, dodeljene tej skupini, bi morale zagotoviti zadostno zastopanost zainteresiranih strani pri delu Agencije. ***Komisija bo glede na pomen certifikacijskih zahtev za zagotovitev zaupanja v internet stvari posebej pretehtala izvedbene ukrepe, s katerimi bi zagotovila uskladitev varnostnih standardov za naprave interneta stvari v vsej EU.***

Predlog spremembe 37

Predlog uredbe
Uvodna izjava 44 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(44a) Agencija bi morala imeti skupino zainteresiranih strani za postopek certificiranja, ki bi delovala kot svetovalni organ, da bi zagotovila redni dialog z zasebnim sektorjem, združenji potrošnikov, znanstveno skupnostjo in drugimi ustreznimi zainteresiranimi stranmi. V skupini zainteresiranih strani za postopek certificiranja, ki jo ustanovi izvršni direktor, bi morali sodelovati splošni svetovalni odbor, ki bi zagotavljal informacije o tem, kateri izdelki in storitve

	IKT bodo zajeti v prihodnjih evropskih certifikacijskih shemah na področju informacijske varnosti, in ad hoc odbori, ki bi prispevali k predlaganju, razvoju in sprejetju zahtevanih evropskih programov za kibernetsko varnost.

Predlog spremembe 38

Predlog uredbe
Uvodna izjava 46

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(46) Da se Agenciji zagotovita popolna samostojnost in neodvisnost ter se ji omogoči, da lahko opravlja dodatne in nove naloge, tudi nepredvidene nujne naloge, bi ji bilo treba dodeliti zadostna lastna proračunska sredstva, ki se večinoma zagotovijo s prispevkom Unije in prispevki tretjih držav, ki sodelujejo pri delu Agencije. Večina osebja Agencije bi morala neposredno sodelovati pri operativnem izvajanju njenega mandata. Državi članici gostiteljici ali vsaki drugi državi članici bi moralo biti dovoljeno, da lahko prostovoljno prispeva k prihodkom Agencije. Za subvencije v breme splošnega proračuna Unije bi se moral še vedno uporabljati postopek za sprejemanje proračuna Unije. Revizijo zaključnih računov Agencije bi moralo opraviti Računsko sodišče, da bi bili zagotovljeni preglednost in ***odgovornost***.	(46) Da se Agenciji zagotovita popolna samostojnost in neodvisnost ter se ji omogoči, da lahko opravlja dodatne in nove naloge, tudi nepredvidene nujne naloge, bi ji bilo treba dodeliti zadostna lastna proračunska sredstva, ki se večinoma zagotovijo s prispevkom Unije in prispevki tretjih držav, ki sodelujejo pri delu Agencije. ***Za zagotovitev, da ima Agencija zadostne zmogljivosti za izpolnjevanje vseh svojih nalog in ciljev, ki jih je vedno več, je ustrezen proračun bistvenega pomen.*** Večina osebja Agencije bi morala neposredno sodelovati pri operativnem izvajanju njenega mandata. Državi članici gostiteljici ali vsaki drugi državi članici bi moralo biti dovoljeno, da lahko prostovoljno prispeva k prihodkom Agencije. Za subvencije v breme splošnega proračuna Unije bi se moral še vedno uporabljati postopek za sprejemanje proračuna Unije. Revizijo zaključnih računov Agencije bi moralo opraviti Računsko sodišče, da bi bili zagotovljeni preglednost***, odgovornost*** in ***učinkovitost porabljenih sredstev***.

Predlog spremembe 39

Predlog uredbe
Uvodna izjava 47

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(47) Ugotavljanje skladnosti pomeni proces ugotavljanja, ali so posebne zahteve glede izdelka, postopka, storitve, sistema, osebe ali organa izpolnjene. Za namene te uredbe bi bilo treba certificiranje šteti za vrsto ugotavljanja skladnosti glede lastnosti izdelka, postopka, storitve, sistema ali kombinacije teh elementov (v nadaljnjem besedilu: izdelki in storitve IKT), povezane s kibernetsko varnostjo, ki ga izvede neodvisna tretja stran, ***ki ni*** proizvajalec izdelka ali ponudnik storitev. Certificiranje samo po sebi ne more jamčiti, da so ***certificirani*** izdelki in storitve IKT kibernetsko varni. Gre bolj za postopek in tehnično metodologijo za potrditev, da so bili izdelki in storitve IKT preskušeni ter da izpolnjujejo nekatere zahteve glede kibernetske varnosti, določene drugje, na primer v tehničnih standardih.	(47) Ugotavljanje skladnosti pomeni proces ugotavljanja, ali so posebne zahteve glede izdelka, postopka, storitve, sistema, osebe ali organa izpolnjene. Za namene te uredbe bi bilo treba certificiranje šteti za vrsto ugotavljanja skladnosti glede lastnosti izdelka, postopka, storitve, sistema ali kombinacije teh elementov (v nadaljnjem besedilu: izdelki***, procesi*** in storitve IKT), povezane s kibernetsko varnostjo, ki ga izvede neodvisna tretja stran ***ali***, ***kadar samoocena to dovoljuje,*** proizvajalec izdelka ali ponudnik storitev. ***Samooceno lahko opravi proizvajalec izdelka, MSP ali ponudnik storitev iz te uredbe in, če je primerno, kot je določeno v novem zakonodajnem okviru in v skladu z njim. Poleg tega jo lahko opravi proizvajalec izdelka ali gospodarski subjekt, kadar ni pričakovati, da bi bila verjetnost incidenta v zvezi s kibernetsko varnostjo in/ali verjetnost, da bo tak incident povzročil resno škodo za družbo ali njen velik del, visoka ali precejšnja, pri čemer se upošteva uporaba zadevnega izdelka ali storitve, i jo je predvidel proizvajalec ali ponudnik storitev.*** Certificiranje samo po sebi ne more jamčiti, da so ***z njim kriti*** izdelki***, procesi*** in storitve IKT kibernetsko varni***, s čimer je treba tudi seznaniti potrošnike in podjetja***. Gre bolj za postopek in tehnično metodologijo za potrditev, da so bili izdelki***, procesi*** in storitve IKT preskušeni ter da izpolnjujejo nekatere zahteve glede kibernetske varnosti, določene drugje, na primer v tehničnih standardih. ***Ti tehnični standardi vključujejo navedbo, ali lahko proizvod, proces ali storitev IKT opravlja svoje redne funkcije brez povezave z internetom.***

Predlog spremembe 40

Predlog uredbe

Uvodna izjava 48

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(48) ***Certificiranje*** kibernetske varnosti ima ***pomembno*** vlogo pri krepitvi zaupanja in varnosti izdelkov in storitev IKT. Enotni digitalni trg, zlasti podatkovno gospodarstvo in internet stvari, lahko uspevajo le, če obstaja splošno zaupanje javnosti, da ti izdelki in storitve nudijo ***določeno*** stopnjo zagotovila kibernetske varnosti. Povezani in avtomatizirani avtomobili, elektronski medicinski pripomočki, nadzorni sistemi industrijske avtomatizacije ter pametna omrežja so le nekateri primeri sektorjev, v katerih je certificiranje že razširjeno ali se bo verjetno uporabljalo v bližnji prihodnosti. Sektorji, ki jih ureja direktiva o varnosti omrežij in informacij, so poleg tega sektorji, v katerih je certificiranje kibernetske varnosti ključnega pomena.	(48) ***Evropsko certificiranje*** kibernetske varnosti ima ***ključno*** vlogo pri krepitvi zaupanja in varnosti izdelkov***, procesov*** in storitev IKT. Enotni digitalni trg, zlasti podatkovno gospodarstvo in internet stvari, lahko uspevajo le, če obstaja splošno zaupanje javnosti, da ti izdelki in storitve nudijo ***visoko*** stopnjo zagotovila kibernetske varnosti. Povezani in avtomatizirani avtomobili, elektronski medicinski pripomočki, nadzorni sistemi industrijske avtomatizacije ter pametna omrežja so le nekateri primeri sektorjev, v katerih je certificiranje že razširjeno ali se bo verjetno uporabljalo v bližnji prihodnosti. Sektorji, ki jih ureja direktiva o varnosti omrežij in informacij, so poleg tega sektorji, v katerih je certificiranje kibernetske varnosti ključnega pomena.

Predlog spremembe 41

Predlog uredbe
Uvodna izjava 49

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(49) V sporočilu „Krepitev odpornosti evropskega sistema kibernetske varnosti ter spodbujanje konkurenčne in inovativne industrije kibernetske varnosti“ iz leta 2016 je Komisija opredelila potrebo po visokokakovostnih, cenovno dostopnih in interoperabilnih izdelkih in rešitvah na področju kibernetske varnosti. Dobava izdelkov IKT in opravljanje storitev IKT na enotnem trgu sta geografsko še vedno zelo razdrobljena. Razlog za to je, da se je industrija kibernetske varnosti v Evropi razvila predvsem zaradi povpraševanja nacionalnih vlad. Poleg tega so med drugimi vrzelmi, ki vplivajo na enotni trg kibernetske varnosti, pomanjkanje interoperabilnih rešitev (tehničnih standardov), praks in vseevropskih	(49) V sporočilu „Krepitev odpornosti evropskega sistema kibernetske varnosti ter spodbujanje konkurenčne in inovativne industrije kibernetske varnosti“ iz leta 2016 je Komisija opredelila potrebo po visokokakovostnih, cenovno dostopnih in interoperabilnih izdelkih in rešitvah na področju kibernetske varnosti. Dobava izdelkov IKT in opravljanje ***procesov in*** storitev IKT na enotnem trgu sta geografsko še vedno zelo razdrobljena. Razlog za to je, da se je industrija kibernetske varnosti v Evropi razvila predvsem zaradi povpraševanja nacionalnih vlad. Poleg tega so med drugimi vrzelmi, ki vplivajo na enotni trg kibernetske varnosti, pomanjkanje interoperabilnih rešitev (tehničnih

mehanizmov certificiranja. Po eni strani evropska podjetja zato težko konkurirajo na nacionalni, evropski in svetovni ravni. Po drugi strani pa se s tem zmanjšuje izbira učinkovitih in uporabnih tehnologij kibernetske varnosti, do katerih imajo dostop državljani in podjetja. Podobno je Komisija v vmesnem pregledu izvajanja strategije za enotni digitalni trg poudarila potrebo po varnih povezanih izdelkih in sistemih ter navedla, da bi z ustanovitvijo evropskega okvira za varnost IKT s pravili za organizacijo varnostnega certificiranja IKT v Uniji lahko ohranili zaupanje v internet in odpravili sedanjo razdrobljenost trga kibernetske varnosti.

standardov), praks in vseevropskih mehanizmov certificiranja. Po eni strani evropska podjetja zato težko konkurirajo na nacionalni, evropski in svetovni ravni. Po drugi strani pa se s tem zmanjšuje izbira učinkovitih in uporabnih tehnologij kibernetske varnosti, do katerih imajo dostop državljani in podjetja. Podobno je Komisija v vmesnem pregledu izvajanja strategije za enotni digitalni trg poudarila potrebo po varnih povezanih izdelkih in sistemih ter navedla, da bi z ustanovitvijo evropskega okvira za varnost IKT s pravili za organizacijo varnostnega certificiranja IKT v Uniji lahko ohranili zaupanje v internet in odpravili sedanjo razdrobljenost trga kibernetske varnosti.

Predlog spremembe 42

Predlog uredbe
Uvodna izjava 50

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(50) Zdaj se certificiranje izdelkov in storitev IKT glede kibernetske varnosti uporablja le v omejenem obsegu. Če obstaja, večinoma poteka na ravni držav članic ali v okviru shem, ki jih usmerja industrija. Tako certifikat, ki ga izda organ za kibernetsko varnost ene države članice, praviloma ni priznan v drugih državah članicah. Tako je možno, da morajo podjetja svoje izdelke in storitve certificirati v več državah članicah, v katerih poslujejo, da bi na primer lahko sodelovala v nacionalnih postopkih javnega naročanja. Poleg tega se zdi, da ni usklajenega in celovitega pristopa k horizontalnim vidikom kibernetske varnosti (npr. na področju interneta stvari), čeprav se pojavljajo nove sheme. Pri obstoječih shemah se pojavljajo znatne pomanjkljivosti in razlike v smislu pokritosti izdelkov, stopenj zagotovila, vsebinskih meril in dejanske uporabe.	(50) Zdaj se certificiranje izdelkov***, procesov*** in storitev IKT glede kibernetske varnosti uporablja le v omejenem obsegu. Če obstaja, večinoma poteka na ravni držav članic ali v okviru shem, ki jih usmerja industrija. Tako certifikat, ki ga izda organ za kibernetsko varnost ene države članice, praviloma ni priznan v drugih državah članicah. Tako je možno, da morajo podjetja svoje izdelke***, procese*** in storitve certificirati v več državah članicah, v katerih poslujejo, da bi na primer lahko sodelovala v nacionalnih postopkih javnega naročanja***, zaradi česar imajo višje stroške***. Poleg tega se zdi, da ni usklajenega in celovitega pristopa k horizontalnim vidikom kibernetske varnosti (npr. na področju interneta stvari), čeprav se pojavljajo nove sheme. Pri obstoječih shemah se pojavljajo znatne pomanjkljivosti in razlike v smislu pokritosti izdelkov, stopenj zagotovila ***na podlagi tveganj***, vsebinskih meril in dejanske uporabe. ***V zvezi s tem je***

	ključnega pomena vzajemno priznavanje in zaupanje med državami članicami. Agencija ENISA ima pomembno vlogo, da državam članicam pomaga razviti trdno institucionalno strukturo in strokovno znanje na področju zaščite pred morebitnimi kibernetskimi napadi. Potreben je pristop za vsak primer posebej, s katerim se zagotovi, da so storitve, procesi in izdelki vključeni v ustrezne certifikacijske sheme. Poleg tega je za učinkovito odkrivanje in blažitev tveganj potreben pristop na podlagi tveganj, obenem pa je treba priznati, da ni mogoče uporabiti sistema enake rešitve za vse.

Predlog spremembe 43

Predlog uredbe
Uvodna izjava 52

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(52) Glede na navedeno je treba vzpostaviti evropski certifikacijski okvir za kibernetsko varnost, ki bi določal glavne horizontalne zahteve za evropske certifikacijske sheme za kibernetsko varnost, ki bi jih bilo treba oblikovati, in omogočal, da bi se certifikati za izdelke in storitve IKT priznavali in uporabljali v vseh državah članicah. Evropski okvir bi moral imeti dvojni cilj: po eni strani naj bi pripomogel k povečanju zaupanja v izdelke in storitve IKT, ki so bili certificirani v skladu s takimi shemami; po drugi strani pa naj bi preprečeval kopičenje nasprotujočih si ali prekrivajočih se nacionalnih certifikacijskih shem za kibernetsko varnost in tako zmanjšal stroške za podjetja, ki poslujejo na enotnem digitalnem trgu. ***Programi*** bi morali biti nediskriminatorni in temeljiti na mednarodnih standardih in/ali standardih Unije, razen če so ti standardi neučinkoviti ali neprimerni za dosego legitimnih ciljev EU v tem oziru.	(52) Glede na navedeno je treba ***sprejeti skupni pristop in*** vzpostaviti evropski certifikacijski okvir za kibernetsko varnost, ki bi določal glavne horizontalne zahteve za evropske certifikacijske sheme za kibernetsko varnost, ki bi jih bilo treba oblikovati, in omogočal, da bi se certifikati za izdelke***, procese*** in storitve IKT priznavali in uporabljali v vseh državah članicah. ***Pri tem je treba nujno temeljiti na obstoječih nacionalnih in mednarodnih shemah ter sistemih vzajemnega priznavanja, zlasti sistemu SOG-IS, pa tudi omogočiti nemoten prehod z obstoječih shem iz teh sistemov na sheme iz novega evropskega okvira.*** Evropski okvir bi moral imeti dvojni cilj: po eni strani naj bi pripomogel k povečanju zaupanja v izdelke***, procese*** in storitve IKT, ki so bili certificirani v skladu s takimi shemami; po drugi strani pa naj bi preprečeval kopičenje nasprotujočih si ali prekrivajočih se nacionalnih certifikacijskih shem za kibernetsko

varnost in tako zmanjšal stroške za podjetja, ki poslujejo na enotnem digitalnem trgu. ***Če evropska certifikacijska shema za kibernetsko varnost nadomesti nacionalno shemo, bi se morali certifikati, izdani v okviru evropske sheme, priznati za veljavne v primerih, ko je bila potrebna certifikacija v okviru nacionalne sheme. Sheme bi morale izhajati iz načela vgrajene varnosti in načel iz Uredbe (EU) 2016/679. Poleg tega bi morale*** biti nediskriminatorni in temeljiti na mednarodnih standardih in/ali standardih Unije, razen če so ti standardi neučinkoviti ali neprimerni za dosego legitimnih ciljev EU v tem oziru.

Predlog spremembe 44

Predlog uredbe
Uvodna izjava 52 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(52a) Evropski certifikacijski okvir za kibernetsko varnost bi moral biti enotno vzpostavljen v vseh državah članicah, da se prepreči praksa „nakupovanja certifikatov“ zaradi razlik v stroških ali stopenj strogosti med državami članicami.

Predlog spremembe 45

Predlog uredbe
Uvodna izjava 52 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(52b) Certifikacijske sheme bi morale temeljiti na že obstoječih sistemih na nacionalni in mednarodni ravni, pri čemer bi se bilo treba opirati na obstoječe pozitivne lastnosti ter ocenjevati in odpravljati pomanjkljivosti.

Predlog spremembe 46

Predlog uredbe
Uvodna izjava 52 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(52c) Prožne rešitve za kibernetsko varnost so nujno potrebne za to, da bi industrija lahko predvidela zlonamerne napade in grožnje, zato bi bilo treba pri vsakršni certifikacijski shemi preprečiti, da bi hitro zastarela.

Predlog spremembe 47

Predlog uredbe
Uvodna izjava 53

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(53) Komisija bi morala biti pooblaščena za sprejemanje evropskih certifikacijskih shem za kibernetsko varnost za določene skupine izdelkov in storitev IKT. Te sheme bi morali izvajati in nadzorovati nacionalni organi za nadzor nad certificiranjem in certifikati, izdani v okviru teh shem, bi morali biti veljavni in priznani po vsej Uniji. Certifikacijske sheme, ki jih izvaja industrija ali druge zasebne organizacije, ne bi smele spadati na področje uporabe te uredbe. Vendar pa lahko organi, ki izvajajo takšne sheme, predlagajo Komisiji, naj preuči možnost, da bi te sheme odobrila kot evropsko shemo.	(53) Komisija bi morala biti pooblaščena za sprejemanje evropskih certifikacijskih shem za kibernetsko varnost za določene skupine izdelkov***, procesov*** in storitev IKT. Te sheme bi morali izvajati in nadzorovati nacionalni organi za nadzor nad certificiranjem in certifikati, izdani v okviru teh shem, bi morali biti veljavni in priznani po vsej Uniji. Certifikacijske sheme, ki jih izvaja industrija ali druge zasebne organizacije, ne bi smele spadati na področje uporabe te uredbe. Vendar pa lahko organi, ki izvajajo takšne sheme, predlagajo Komisiji, naj preuči možnost, da bi te sheme odobrila kot evropsko shemo. ***Agencija bi morala opredeliti in oceniti sheme, ki se že uporabljajo v industriji ali zasebnih organizacijah, da bi izbrala najboljšo prakso, ki bi lahko postala del evropske sheme. Akterji v industriji lahko pred certificiranjem opravijo samooceno svojih izdelkov ali storitev in tako pokažejo, da je njihov izdelek ali storitev pripravljen na postopek certificiranja, če bi bil zahtevan ali potreben.***

Predlog spremembe 48

Predlog uredbe
Uvodna izjava 53 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(53a) Agencija in Komisija bi morali čim bolje uporabiti obstoječe certifikacijske sheme na ravni EU in/ali mednarodni ravni. Agencija ENISA bi morala biti sposobna oceniti, katere sheme, ki se že uporabljajo, ustrezajo svojemu namenu in jih je mogoče vključiti v evropsko zakonodajo v sodelovanju z organizacijami EU za standardizacijo in, kolikor je to mogoče, mednarodno priznati. Obstoječe primere dobre prakse bi bilo treba zbrati in deliti med državami članicami.

Predlog spremembe 49

Predlog uredbe
Uvodna izjava 54

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(54) Določbe te uredbe ne bi smele posegati v zakonodajo Unije, ki vsebuje posebne predpise o certificiranju izdelkov in storitev IKT. Zlasti Splošna uredba o varstvu podatkov vsebuje določbe za uvedbo certifikacijskih mehanizmov ter pečatov in označb za varstvo podatkov, katerih namen je dokazovanje, da so postopki obdelave, ki jih uporabljajo upravljavci in obdelovalci, skladni z navedeno uredbo. Taki certifikacijski mehanizmi ter pečati in označbe za varstvo podatkov bi morali posameznikom, na katere se podatki nanašajo, omogočati, da hitro ocenijo raven varstva podatkov zadevnih izdelkov in storitev. Ta uredba ne posega v certificiranje postopkov obdelave podatkov na podlagi Splošne uredbe o varstvu podatkov, tudi kadar so taki postopki vgrajeni v izdelke in storitve.	(54) Določbe te uredbe ne bi smele posegati v zakonodajo Unije, ki vsebuje posebne predpise o certificiranju izdelkov***, procesov*** in storitev IKT. Zlasti Splošna uredba o varstvu podatkov vsebuje določbe za uvedbo certifikacijskih mehanizmov ter pečatov in označb za varstvo podatkov, katerih namen je dokazovanje, da so postopki obdelave, ki jih uporabljajo upravljavci in obdelovalci, skladni z navedeno uredbo. Taki certifikacijski mehanizmi ter pečati in označbe za varstvo podatkov bi morali posameznikom, na katere se podatki nanašajo, omogočati, da hitro ocenijo raven varstva podatkov zadevnih izdelkov in storitev. Ta uredba ne posega v certificiranje postopkov obdelave podatkov na podlagi Splošne uredbe o varstvu podatkov, tudi kadar so taki postopki vgrajeni v izdelke in storitve.

Predlog spremembe 50

Predlog uredbe
Uvodna izjava 55

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(55) Evropske certifikacijske sheme za kibernetsko varnost bi morale zagotoviti, da izdelki in ***storitve*** IKT, certificirani v taki shemi, izpolnjujejo navedene zahteve. Takšne zahteve se nanašajo na zmožnost za odpornost, na določeni stopnji ***zagotovila***, na dejanja, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti in zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali z njimi povezanih funkcij ali storitev, ki jih ponujajo ali so dostopni prek navedenih izdelkov, postopkov, storitev in sistemov v smislu te uredbe. V tej uredbi ni mogoče podrobno določiti zahtev glede kibernetske varnosti, ki se nanašajo na vse izdelke in ***storitve*** IKT. Izdelki in ***storitve*** IKT ter s tem povezane potrebe po kibernetski varnosti so tako raznoliki, da je zelo težko oblikovati splošne zahteve glede kibernetske varnosti, ki bi veljale na vseh področjih. Zato je treba sprejeti širok in splošen pojem kibernetske varnosti za namene certificiranja, ki ga dopolnjuje sklop posebnih ciljev za kibernetsko varnost, ki jih je treba upoštevati pri oblikovanju evropskih certifikacijskih shem za kibernetsko varnost. Kako bodo takšni cilji doseženi pri posameznih izdelkih in ***storitvah*** IKT, bi bilo treba nadalje podrobno opredeliti na ravni posamezne certifikacijske sheme, ki jo sprejme Komisija, npr. s sklicem na standarde ali tehnične specifikacije.	(55) Evropske certifikacijske sheme za kibernetsko varnost bi morale zagotoviti, da izdelki***, storitve*** in ***procesi*** IKT, certificirani v taki shemi, izpolnjujejo navedene zahteve. Takšne zahteve se nanašajo na zmožnost za odpornost, na določeni stopnji ***tveganja***, na dejanja, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti in zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali z njimi povezanih funkcij ali storitev, ki jih ponujajo ali so dostopni prek navedenih izdelkov, postopkov, storitev in sistemov v smislu te uredbe. V tej uredbi ni mogoče podrobno določiti zahtev glede kibernetske varnosti, ki se nanašajo na vse izdelke***, storitve*** in ***procese*** IKT. Izdelki***, storitve*** in ***procesi*** IKT ter s tem povezane potrebe po kibernetski varnosti so tako raznoliki, da je zelo težko oblikovati splošne zahteve glede kibernetske varnosti, ki bi veljale na vseh področjih. Zato je treba sprejeti širok in splošen pojem kibernetske varnosti za namene certificiranja, ki ga dopolnjuje sklop posebnih ciljev za kibernetsko varnost, ki jih je treba upoštevati pri oblikovanju evropskih certifikacijskih shem za kibernetsko varnost. Kako bodo takšni cilji doseženi pri posameznih izdelkih***, storitvah*** in ***procesih*** IKT, bi bilo treba nadalje podrobno opredeliti na ravni posamezne certifikacijske sheme, ki jo sprejme Komisija, npr. s sklicem na standarde ali tehnične specifikacije. ***Vse akterje, ki so vključeni v dobavno verigo, bi bilo treba spodbujati, da razvijejo in sprejmejo varnostne in tehnične standarde ter načelo vgrajene varnosti v vseh fazah življenjskega cikla izdelka, storitve ali postopka; vsaka evropska certifikacijska shema za kibernetsko varnost bi morala biti oblikovana tako, da***

bi pokrivala to področje uporabe.

Predlog spremembe 51

Predlog uredbe
Uvodna izjava 56

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(56) Komisijo bi morali pooblastiti, da od agencije ENISA zahteva, naj pripravi predloge za sheme za posamezne izdelke ali storitve IKT. Nadalje bi morali Komisijo pooblastiti, da ***na podlagi*** predloge za shemo, ki jo predlaga agencija ENISA, sprejme ***evropsko certifikacijsko shemo*** za kibernetsko varnost z ***izvedbenimi*** akti. Ob upoštevanju splošnega namena in varnostnih ciljev, opredeljenih v tej uredbi, bi moral biti v evropskih certifikacijskih shemah za kibernetsko varnost***, ki jih sprejme Komisija,*** opredeljen minimalni sklop elementov v zvezi z vsebino, področjem uporabe in delovanjem posamezne sheme. Sklop bi moral med drugim vključevati področje uporabe in predmet certificiranja kibernetske varnosti, vključno z zajetimi kategorijami izdelkov in storitev IKT, podrobno specifikacijo zahtev glede kibernetske varnosti, npr. s sklicem na standarde ali tehnične specifikacije, posebnimi merili in metodami za ocenjevanje ter predvideno stopnjo zagotovila – osnovno, znatno in/ali visoko.	(56) Komisijo bi morali pooblastiti, da od agencije ENISA zahteva, naj pripravi predloge za sheme za posamezne izdelke***, procese*** ali storitve IKT ***na podlagi upravičenih razlogov, in sicer da obstoječe nacionalne certifikacijske sheme za kibernetsko varnost povzročajo razdrobljenost notranjega trga; da obstaja potreba po podpori pravu Unije ali če se taka potreba pričakuje; da skupina držav članic za certificiranje ali skupina zainteresiranih strani za certificiranje izda mnenje.*** Nadalje bi morali Komisijo pooblastiti, da ***po oceni*** predloge za ***certifikacijsko*** shemo, ki jo predlaga agencija ENISA ***na podlagi zahteve Komisije***, sprejme ***evropske certifikacijske sheme*** za kibernetsko varnost z ***delegiranimi*** akti. Ob upoštevanju splošnega namena in varnostnih ciljev, opredeljenih v tej uredbi, bi moral biti v ***teh*** evropskih certifikacijskih shemah za kibernetsko varnost opredeljen minimalni sklop elementov v zvezi z vsebino, področjem uporabe in delovanjem posamezne sheme. Sklop bi moral med drugim vključevati področje uporabe in predmet certificiranja kibernetske varnosti, vključno z zajetimi kategorijami izdelkov in storitev IKT, podrobno specifikacijo zahtev glede kibernetske varnosti, npr. s sklicem na standarde ali tehnične specifikacije, posebnimi merili in metodami za ocenjevanje ter predvideno stopnjo zagotovila – osnovno, znatno in/ali visoko.

Predlog spremembe 52

Predlog uredbe
Uvodna izjava 56 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(56a) Agencija bi morala biti referenčna točka za informacije o evropskih shemah kibernetske varnosti. Vzdrževati bi morala spletno stran z vsemi pomembnimi informacijami, vključno z informacijami o umaknjenih in poteklih certifikatih in nacionalnih certifikatih, ki jih pokriva. Agencija bi morala zagotoviti, da je ustrezni del vsebine njene spletne strani razumljiv za običajne potrošnike.

Predlog spremembe 53

Predlog uredbe
Uvodna izjava 56 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(56b) Določanje stopenj zagotovila za certifikate je potrebno za to, da se končnemu uporabniku predstavi, katere pričakovane vrste kibernetskih groženj nameravajo ukrepi kibernetske varnosti v izdelku, postopku ali storitvi preprečiti. Kibernetske grožnje je treba opredeliti ob upoštevanju pričakovanega tveganja in zmogljivosti storilca ali storilcev napada glede na pričakovano uporabe zajetega izdelka, procesa ali storitve IKT. Osnovna stopnja zagotovila pomeni sposobnost preprečevanja napadov, katerim se je mogoče izogniti z osnovnimi ukrepi kibernetske varnosti in jih je mogoče enostavno preveriti s pregledom tehnične dokumentacije. Znatna stopnja zagotovila se nanaša na sposobnost preprečevanja znanih vrst napadov napadalca z določeno stopnjo izpopolnjenosti, vendar z omejenimi viri. Visoka stopnja zagotovila se nanaša na zmogljivost za odpornost zoper neznane ranljivosti in izpopolnjene napade z najsodobnejšimi tehnologijami in znatnimi viri, kot so financirane

multidisciplinarne skupine.

Predlog spremembe 54

Predlog uredbe
Uvodna izjava 56 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(56c) Da bi se izognili razdrobljenosti notranjega trga zaradi nacionalnih sistemov za kibernetsko varnost, podprli prihodnjo zakonodajo ter povečali zaupanje in varnost, bi bilo treba na Komisijo prenesti pooblastila, da v skladu s členom 290 Pogodbe o delovanju Evropske unije sprejme akte v zvezi z določanjem prednostnih nalog za evropsko certificiranje kibernetske varnosti, sprejetjem tekočega programa in sprejetjem evropskih certifikacijskih shem. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016. Da bi zagotovila enakopravno sodelovanje pri pripravi delegiranih aktov, bi Evropski parlament in Svet morala prejeti vse dokumente istočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa bi morali imeti možnost, da se sistematično udeležujejo sej strokovnih skupin Komisije, ki se ukvarjajo s pripravo delegiranih aktov.

Predlog spremembe 55

Predlog uredbe
Uvodna izjava 56 d (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(56d) Med metodami za ocenjevanje in postopki ocenjevanja, povezanimi s posamezno evropsko certifikacijsko shemo

	za kibernetsko varnost, bi bilo treba na ravni Unije spodbujati etično vdiranje, katerega namen je odkrivanje pomanjkljivosti in šibkih točk naprav in informacijskih sistemov s predvidevanjem načrtovanih dejanj in spretnosti zlonamernih hekerjev.

Predlog spremembe 56

Predlog uredbe
Uvodna izjava 57

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(57) Uporaba evropskega certificiranja kibernetske varnosti bi morala ostati prostovoljna, razen če je v zakonodaji Unije ali nacionalni zakonodaji določeno drugače. Da pa bi dosegli cilje te uredbe in preprečili razdrobljenost notranjega trga, bi nacionalne certifikacijske sheme ali postopki za kibernetsko varnost za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, morali prenehati učinkovati od datuma, ki ga določi Komisija z ***izvedbenim*** aktom. Poleg tega države članice ne bi smele uvajati novih nacionalnih certifikacijskih shem, ki bi določale certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT, ki jih že zajema obstoječa evropska certifikacijska shema za kibernetsko varnost.	(57) Uporaba evropskega certificiranja kibernetske varnosti bi morala ostati prostovoljna, razen če je v zakonodaji Unije ali nacionalni zakonodaji določeno drugače. Da pa bi dosegli cilje te uredbe in preprečili razdrobljenost notranjega trga, bi nacionalne certifikacijske sheme ali postopki za kibernetsko varnost za izdelke***, procese*** in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, morali prenehati učinkovati od datuma, ki ga določi Komisija z ***delegiranim*** aktom. Poleg tega države članice ne bi smele uvajati novih nacionalnih certifikacijskih shem, ki bi določale certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT, ki jih že zajema obstoječa evropska certifikacijska shema za kibernetsko varnost. ***Vendar pa ta uredba ne bi smela posegati v nacionalne sheme, za katere so izključno pristojne države članice in ki zadevajo izdelke, procese in storitve IKT, ki se uporabljajo za potrebe držav članic na tem področju.***

Predlog spremembe 57

Predlog uredbe
Uvodna izjava 57 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(57c) Uvede se dolžnost, da se za izdelek izda izjava, ki vsebuje strukturirane informacije v zvezi s certificiranjem izdelka, procesa ali storitve, iz katere lahko potrošnik razbere več informacij in se na njihovi podlagi odloči za nakup.

Predlog spremembe 58

Predlog uredbe
Uvodna izjava 57 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(57b) Pri predlaganju novih evropskih shem za kibernetsko varnost bi morali ENISA in drugi zadevni organi ustrezno pozornost nameniti konkurenčni dinamiki predloga, pri tem pa zlasti zagotoviti, da v primeru, ko ima zadevni sektor veliko malih in srednjih podjetij, na primer pri razvoju programske opreme, sheme certificiranja niso ovira za vstop novih podjetij in inovacij.

Predlog spremembe 59

Predlog uredbe
Uvodna izjava 57 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(57c) Evropske sheme za kibernetsko varnost bodo pomagale uskladiti in poenotiti prakso na področju kibernetske varnosti v Uniji. Vendar pa ne smejo postati najnižja raven kibernetske varnosti. Pri zasnovi evropskih shem kibernetske varnosti bi bilo treba tudi upoštevati in omogočiti razvoj novih inovacij na področju kibernetske varnosti.

Predlog spremembe 60

Predlog uredbe
Uvodna izjava 58

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(58) Ko bo sprejeta evropska certifikacijska shema za kibernetsko varnost, bi morali proizvajalci izdelkov IKT ali ponudniki storitev IKT imeti možnost, da vložijo vlogo za certificiranje svojih izdelkov ali storitev pri organu za ugotavljanje skladnosti po lastni izbiri. Organe za ugotavljanje skladnosti bi moral akreditirati akreditacijski organ, če izpolnjujejo nekatere posebne zahteve, določene v tej uredbi. Akreditacija bi morala biti izdana za obdobje največ petih let in bi se lahko pod enakimi pogoji podaljšala, če bi organ za ugotavljanje skladnosti izpolnjeval določene zahteve. Akreditacijski organi bi morali preklicati akreditacijo organa za ugotavljanje skladnosti, če pogoji za akreditacijo niso ali niso več izpolnjeni ali če ukrepi, ki jih sprejme organ za ugotavljanje skladnosti, kršijo to uredbo.	(58) Ko bo sprejeta evropska certifikacijska shema za kibernetsko varnost, bi morali proizvajalci izdelkov IKT ali ponudniki ***procesov ali*** storitev IKT imeti možnost, da vložijo vlogo za certificiranje svojih izdelkov ali storitev pri organu za ugotavljanje skladnosti po lastni izbiri ***kjerkoli v Uniji***. Organe za ugotavljanje skladnosti bi moral akreditirati akreditacijski organ, če izpolnjujejo nekatere posebne zahteve, določene v tej uredbi. Akreditacija bi morala biti izdana za obdobje največ petih let in bi se lahko pod enakimi pogoji podaljšala, če bi organ za ugotavljanje skladnosti izpolnjeval določene zahteve. Akreditacijski organi bi morali preklicati akreditacijo organa za ugotavljanje skladnosti, če pogoji za akreditacijo niso ali niso več izpolnjeni ali če ukrepi, ki jih sprejme organ za ugotavljanje skladnosti, kršijo to uredbo. ***Agencija bi morala izvajati preglede za zagotovitev enakovredne ravni kakovosti in skrbnosti in vestnosti organov za ugotavljanje skladnosti, da bi preprečili regulativno arbitražo. Rezultate bi bilo treba poročati agenciji, Komisiji in Parlamentu ter jih dati na voljo javnosti.***

Predlog spremembe 61

Predlog uredbe
Uvodna izjava 58 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(58a) Obvezna uporaba evropskega certificiranja kibernetske varnosti bi morala biti omejena na primere, ko analiza tveganja upravičuje stroške za industrijo, državljane in potrošnike. Incidenti, ki zmotijo bistvene storitve, lahko ovirajo gospodarske dejavnosti,

	ustvarjajo znatne finančne izgube, slabijo zaupanje uporabnikov in povzročajo veliko škodo gospodarstvu Unije. Obvezna uporaba evropskega certificiranja kibernetske varnosti za izvajalce bistvenih storitev bi morala biti omejena na tiste elemente, ki so kritični za delovanje in se ne bi smela uporabljati za izdelke, procese in storitve splošnega namena, pri katerih bi lahko nastali neutemeljeni stroški za industrijo in potrošnike. Komisija bi morala sodelovati s skupino za sodelovanje, vzpostavljeno v skladu s členom 11 Direktive (EU) 2016/1148, da bi oblikovala seznam kategorij izdelkov, procesov in storitev, ki so izrecno namenjeni za uporabo izvajalcev bistvenih storitev in katerih nepravilno delovanje ob incidentu bi lahko znatno moteče za bistveno storitev. Ta seznam bi bilo treba sestaviti postopoma in ga po potrebi posodabljati. Samo izdelki, procesi in storitve na tem seznamu bi morali biti obvezni za izvajalce bistvenih storitev.

Predlog spremembe 62

Predlog uredbe
Uvodna izjava 58 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(58b) Navzkrižna sklicevanja v nacionalni zakonodaji, ki se sklicujejo na nacionalni standard, ki več ni pravno veljaven zaradi začetka veljavnosti evropske certifikacijske sheme, je lahko potencialni vir zmede za proizvajalce in končne uporabnike. Da bi proizvajalcem preprečile nadaljnje izvajanje specifikacij, ki ustrezajo nacionalnim certifikatom, ki več niso veljavni, bi morale države članice v skladu s svojimi obveznostmi iz Pogodb prilagoditi nacionalno zakonodajo, da bo odražala sprejetje evropske certifikacijske sheme.

Predlog spremembe 63

Predlog uredbe
Uvodna izjava 59

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(59) Od vseh držav članic je treba zahtevati, naj določijo en organ za nadzor nad certificiranjem kibernetske varnosti, ki bi nadzoroval skladnost organov za ugotavljanje skladnosti in certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz te uredbe in ustreznih certifikacijskih shem za kibernetsko varnost. Nacionalni organi za nadzor nad certificiranjem bi morali obravnavati pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, v ustreznem obsegu preučiti vsebino pritožbe ter pritožnika v razumnem roku obvestiti o napredku in izidih preiskave. Poleg tega bi morali sodelovati z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih shem za kibernetsko varnost.	(59) Od vseh držav članic je treba zahtevati, naj določijo en organ za nadzor nad certificiranjem kibernetske varnosti, ki bi nadzoroval skladnost organov za ugotavljanje skladnosti in certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz te uredbe in ustreznih certifikacijskih shem za kibernetsko varnost***, ter naj zagotovijo priznavanje evropskih certifikatov za kibernetsko varnost na njihovem ozemlju***. Nacionalni organi za nadzor nad certificiranjem bi morali obravnavati pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem ***na njihovem ozemlju, ali v zvezi z domnevnim nepriznavanjem certifikatov*** na njihovem ozemlju, v ustreznem obsegu preučiti vsebino pritožbe ter pritožnika v razumnem roku obvestiti o napredku in izidih preiskave. Poleg tega bi morali sodelovati z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov***, procesov*** in storitev IKT z zahtevami iz te uredbe ali posebnih shem za kibernetsko varnost***, ali nepriznavanju evropskih certifikatov za kibernetsko varnost***. Prav tako bi morali nadzorovati lastne izjave o skladnosti in preverjati njihovo skladnost ter ali so evropske certifikate kibernetske varnosti izdali organi za ugotavljanje skladnosti z zahtevami, določenimi v tej uredbi, vključno s pravili, ki jih je sprejela Evropska certifikacijska skupina za kibernetsko varnost, in zahtevami, določenimi v ustrezni evropski certifikacijski shemi za kibernetsko varnost. Za ustrezno izvajanje evropskih certifikacijskih shem za kibernetsko

	varnost in reševanje tehničnih vprašanj o kibernetski varnosti izdelkov in storitev IKT je ključnega pomena učinkovito sodelovanje med nacionalnimi organi za nadzor nad certificiranjem. Komisija bi morala to izmenjavo informacij omogočiti z vzpostavitvijo splošnega elektronskega sistema informacijske podpore, na primer informacijskega in komunikacijskega sistema za nadzor trga (ICSMS) ter sistema hitrega obveščanja o nevarnih neživilskih izdelkih (RAPEX), ki ju organi za nadzor trga že uporabljajo v skladu z Uredbo (ES) št. 765/2008.

Predlog spremembe 64

Predlog uredbe
Uvodna izjava 60

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(60) Da bi zagotovili dosledno uporabo evropskega certifikacijskega okvira za kibernetsko varnost, bi bilo treba ustanoviti ***Evropsko*** certifikacijsko skupino ***za kibernetsko varnost (v nadaljnjem besedilu: skupina)***, ki bi jo sestavljali nacionalni organi za nadzor nad certificiranjem. Glavne naloge skupine bi morale biti svetovati in pomagati Komisiji pri njenih prizadevanjih za zagotovitev doslednega izvajanja in uporabe evropskega certifikacijskega okvira za kibernetsko varnost; pomagati in tesno sodelovati z Agencijo pri pripravi predlog za certifikacijske sheme za kibernetsko varnost; predlagati, da Komisija od Agencije zahteva, naj pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost; in sprejeti mnenja, naslovljena na Komisijo, glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost.	(60) Da bi zagotovili dosledno uporabo evropskega certifikacijskega okvira za kibernetsko varnost, bi bilo treba ustanoviti certifikacijsko skupino ***držav članic***, ki bi jo sestavljali nacionalni organi za nadzor nad certificiranjem. Glavne naloge ***certifikacijske*** skupine ***držav članic*** bi morale biti svetovati in pomagati Komisiji pri njenih prizadevanjih za zagotovitev doslednega izvajanja in uporabe evropskega certifikacijskega okvira za kibernetsko varnost; pomagati in tesno sodelovati z Agencijo pri pripravi predlog za certifikacijske sheme za kibernetsko varnost; predlagati, da Komisija od Agencije zahteva, naj pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost; in sprejeti mnenja, naslovljena na Komisijo, glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost.

Predlog spremembe 65

Predlog uredbe
Uvodna izjava 60 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(60a) Da se zagotovi enakovredna raven usposobljenosti organov za ugotavljanje skladnosti, olajša vzajemno priznavanje ter spodbudi splošno sprejemanje certifikatov o in rezultatov ugotavljanja skladnosti, ki jih izdajajo organi za ocenjevanje skladnosti, morajo nacionalni organi za nadzor nad certificiranjem izvajati strog in pregleden sistem medsebojnih strokovnih pregledov ter redno opravljati take preglede.

Predlog spremembe 66

Predlog uredbe
Uvodna izjava 60 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(60b) Učinkovito sodelovanje med nacionalnimi organi za nadzor nad certificiranjem je bistvenega pomena za pravilno izvajanje medsebojnih strokovnih pregledov in za čezmejno akreditacijo. Zaradi preglednosti je torej treba določiti obveznost nacionalnih organov za nadzor nad certificiranjem za medsebojno izmenjavo informacij ter zagotavljati ustrezne informacije nacionalnim organom in Komisiji. Ažurne in točne informacije o razpoložljivosti akreditacijskih dejavnosti, ki jih opravljajo nacionalni akreditacijski organi, bi bilo treba tudi objaviti in torej dati na voljo zlasti organom za ugotavljanje skladnosti.

Predlog spremembe 67

Predlog uredbe
Uvodna izjava 61

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(61) Da bi Evropska komisija okrepila ozaveščenost in olajšala sprejemljivost prihodnjih shem EU za kibernetsko varnost, lahko izda splošne ali sektorske smernice za kibernetsko varnost, npr. o dobrih praksah ali odgovornem ravnanju na področju kibernetske varnosti, pri čemer poudari pozitivni učinek uporabe certificiranih izdelkov in storitev IKT.	(61) Da bi Evropska komisija okrepila ozaveščenost in olajšala sprejemljivost prihodnjih shem EU za kibernetsko varnost, lahko izda splošne ali sektorske smernice za kibernetsko varnost, npr. o dobrih praksah ali odgovornem ravnanju na področju kibernetske varnosti, pri čemer poudari pozitivni učinek uporabe certificiranih izdelkov***, procesov*** in storitev IKT.

Predlog spremembe 68

Predlog uredbe
Uvodna izjava 63

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(63) Da bi lahko podrobneje opredelili merila za akreditacijo organov za ugotavljanje skladnosti, bi bilo treba Komisijo pooblastiti za sprejetje aktov v skladu s členom 290 Pogodbe o delovanju Evropske unije. Komisija bi morala med pripravami izvesti ustrezna posvetovanja, vključno s posvetovanji na strokovni ravni. Ta posvetovanja bi morala potekati v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016. Da bi zagotovila enakopravno sodelovanje pri pripravi delegiranih aktov, bi Evropski parlament in Svet morala prejeti vse dokumente istočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa bi morali imeti možnost, da se sistematično udeležujejo sej strokovnih skupin Komisije, ki se ukvarjajo s pripravo delegiranih aktov.	(63) Da bi lahko podrobneje opredelili merila za akreditacijo organov za ugotavljanje skladnosti, bi bilo treba Komisijo pooblastiti za sprejetje aktov v skladu s členom 290 Pogodbe o delovanju Evropske unije. Komisija bi morala med pripravami izvesti ustrezna posvetovanja, vključno s posvetovanji na strokovni ravni ***in po potrebi z ustreznimi deležniki***. Ta posvetovanja bi morala potekati v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016. Da bi zagotovila enakopravno sodelovanje pri pripravi delegiranih aktov, bi Evropski parlament in Svet morala prejeti vse dokumente istočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa bi morali imeti možnost, da se sistematično udeležujejo sej strokovnih skupin Komisije, ki se ukvarjajo s pripravo delegiranih aktov.

Predlog spremembe 69

Predlog uredbe
Uvodna izjava 65

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(65) ***Postopek pregleda*** bi bilo treba uporabiti za sprejetje izvedbenih aktov o evropskih certifikacijskih shemah za kibernetsko varnost za izdelke in storitve IKT**,** o načinih izvajanja preiskav s strani Agencije ter o okoliščinah, oblikah in postopkih priglasitve akreditiranih organov za ugotavljanje skladnosti Komisiji s strani nacionalnih organov za nadzor nad certificiranjem.	(65) ***Delegirane akte*** bi bilo treba ***poleg tega*** uporabiti za sprejetje izvedbenih aktov o evropskih certifikacijskih shemah za kibernetsko varnost za izdelke***, procese*** in storitve IKT o načinih izvajanja preiskav s strani Agencije ter o okoliščinah, oblikah in postopkih priglasitve akreditiranih organov za ugotavljanje skladnosti Komisiji s strani nacionalnih organov za nadzor nad certificiranjem.

Predlog spremembe 70

Predlog uredbe
Uvodna izjava 66

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(66) Dejavnosti Agencije bi bilo treba ***oceniti*** neodvisno. Pri oceni bi bilo treba upoštevati doseganje ciljev s strani Agencije, njeno delovno prakso in relevantnost njenih nalog. Oceniti ***pa*** bi ***bilo treba tudi učinek, uspešnost in učinkovitost evropskega certifikacijskega okvira*** za ***kibernetsko varnost***.	(66) Dejavnosti Agencije bi bilo treba ***stalno in*** neodvisno ***ocenjevati***. Pri oceni bi bilo treba upoštevati doseganje ciljev s strani Agencije, njeno delovno prakso in relevantnost njenih nalog***, zlasti njeno usklajevalno vlogo v odnosu do držav članic in njihovih nacionalnih organov***. ***V primeru pregleda bi morala Komisija*** oceniti ***možnost, da*** bi ***agencija delovala kot enotna kontaktna točka „vse na enem mestu“*** za ***države članice ter organe in institucije Unije***.

Predlog spremembe 71

Predlog uredbe
Uvodna izjava 66 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(66a) Oceniti pa bi bilo treba tudi učinek, uspešnost in učinkovitost evropskega certifikacijskega okvira za kibernetsko varnost. V primeru pregleda bi lahko Komisija ocenila vlogo agencije pri ocenjevanju izdelkov in storitev iz tretjih

držav, ki vstopajo na trg Unije, ter možnost uvrščanja podjetij, ki ne spoštujejo predpisov Unije, na črni seznam.

Predlog spremembe 72

Predlog uredbe
Uvodna izjava 66 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(66b) Ocena bi morala analizirati raven kibernetske varnosti izdelkov in storitev, ki se prodajajo v Uniji. V primeru pregleda bi morala Komisija oceniti, ali naj bistvene zahteve na področju kibernetske varnosti vključi kot pogoj za dostop na notranji trg.

Predlog spremembe 73

Predlog uredbe
Člen 1 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) določa cilje, naloge in organizacijske vidike Agencije ***EU za kibernetsko*** varnost ENISA (v nadaljnjem besedilu: Agencija) ter	(a) določa cilje, naloge in organizacijske vidike Agencije ***Evropske unije za*** varnost ***omrežij in informacij*** ENISA (v nadaljnjem besedilu: Agencija) ter

Predlog spremembe 74

Predlog uredbe
Člen 1 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) določa okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za zagotavljanje ustrezne ravni kibernetske varnosti izdelkov in storitev IKT v Uniji***. Ta okvir*** se uporablja brez poseganja v posebne določbe glede prostovoljnega ***ali***	(b) določa okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za ***preprečevanje razdrobljenosti certifikacijskih shem v Uniji in*** zagotavljanje ustrezne ravni kibernetske varnosti izdelkov***, procesov*** in storitev IKT v Uniji***, ki*** se uporablja brez

obveznega certificiranja v drugih aktih Unije.	poseganja v posebne določbe glede prostovoljnega ***in, kjer je ustrezno,*** obveznega certificiranja***, kadar je to določeno v tej uredbi ali*** v drugih aktih Unije.

Predlog spremembe 75

Predlog uredbe
Člen 1 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Agencija izvaja svoje naloge brez poseganja v pristojnosti držav članic na področju kibernetske varnosti in zlasti pristojnosti držav članic na področju javne varnosti, obrambe, državne varnosti in kazenskega prava.

Predlog spremembe 76

Predlog uredbe
Člen 2 – odstavek 1 – točka 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) „kibernetska varnost“ ***zajema*** vse dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, njihovih uporabnikov in prizadetih oseb pred kibernetskimi grožnjami;	(1) „kibernetska varnost“ ***pomeni*** vse dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, njihovih uporabnikov in prizadetih oseb pred kibernetskimi grožnjami;

Predlog spremembe 77

Predlog uredbe
Člen 2 – odstavek 1 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) „omrežje in informacijski sistem“ pomeni sistem, kot je opredeljen v točki (1) člena 4 Direktive (EU) 2016/1148;	(2) „omrežje in informacijski sistem“ pomeni ***omrežje in informacijski*** sistem, kot je opredeljen v točki (1) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 78

Predlog uredbe
Člen 2 – odstavek 1 – točka 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) „nacionalna strategija za varnost omrežij in informacijskih sistemov“ pomeni ***okvir***, kot je ***opredeljen*** v točki (3) člena 4 Direktive (EU) 2016/1148;	(3) „nacionalna strategija za varnost omrežij in informacijskih sistemov“ pomeni ***nacionalno strategijo za varnost omrežij in informacijskih sistemov***, kot je ***opredeljena*** v točki (3) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 79

Predlog uredbe
Člen 2 – odstavek 1 – točka 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) „izvajalec bistvenih storitev“ pomeni ***javni ali zasebni subjekt***, kot je opredeljen v točki (4) člena 4 Direktive (EU) 2016/1148;	(4) „izvajalec bistvenih storitev“ pomeni ***izvajalca bistvenih storitev***, kot je opredeljen v točki (4) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 80

Predlog uredbe
Člen 2 – odstavek 1 – točka 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(5) „ponudnik digitalnih storitev“ pomeni ***vsako pravno osebo, ki zagotavlja digitalno*** storitev, kot je ***opredeljena*** v točki (6) člena 4 Direktive (EU) 2016/1148;	(5) „ponudnik digitalnih storitev“ pomeni ***ponudnika digitalnih*** storitev, kot je ***opredeljen*** v točki (6) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 81

Predlog uredbe
Člen 2 – odstavek 1 – točka 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(6) „incident“ pomeni ***vsak dogodek***, kot	(6) „incident“ pomeni ***incident***, kot je

je opredeljen v točki (7) člena 4 Direktive (EU) 2016/1148;	opredeljen v točki (7) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 82

Predlog uredbe
Člen 2 – odstavek 1 – točka 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) „obvladovanje incidentov“ pomeni ***vsak postopek***, kot je ***opredeljen*** v točki (8) člena 4 Direktive (EU) 2016/1148;	(7) „obvladovanje incidentov“ pomeni ***obvladovanje incidentov***, kot je ***opredeljeno*** v točki (8) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 83

Predlog uredbe
Člen 2 – odstavek 1 – točka 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(8) „kibernetska grožnja“ pomeni vsako potencialno okoliščino ali dogodek, ki bi lahko škodljivo vplival na omrežja in informacijske sisteme, njihove uporabnike in prizadete osebe;	(8) „kibernetska grožnja“ pomeni vsako potencialno okoliščino ali dogodek ***ali vsako namerno dejanje, tudi avtomatiziran ukaz***, ki bi lahko ***poškodoval, prekinil ali drugače*** škodljivo vplival na omrežja in informacijske sisteme, njihove uporabnike in prizadete osebe;

Predlog spremembe 84

Predlog uredbe
Člen 2 – odstavek 1 – točka 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(8a) „kibernetska higiena“ pomeni preproste in rutinske ukrepe, ki zmanjšajo izpostavljenost uporabnikov in podjetij tveganjem zaradi kibernetskih groženj, kadar jih ti uporabniki in podjetja redno izvajajo in uporabljajo na spletu.

Predlog spremembe 85

Predlog uredbe
Člen 2 – odstavek 1 – točka 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) „evropska certifikacijska shema za kibernetsko varnost“ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so opredeljeni na ravni Unije in se uporabljajo za certificiranje izdelkov in ***storitev*** informacijske in komunikacijske tehnologije (IKT), ki spadajo na področje uporabe določene sheme;	(9) „evropska certifikacijska shema za kibernetsko varnost“ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so opredeljeni na ravni Unije in ***usklajeni z mednarodnimi in evropskimi standardi in specifikacijami IKT, ki jih je odobrila agencija ENISA, in*** se uporabljajo za certificiranje izdelkov***,*** ***storitev*** in ***procesov*** informacijske in komunikacijske tehnologije (IKT), ki spadajo na področje uporabe določene sheme;

Predlog spremembe 86

Predlog uredbe
Člen 2 – odstavek 1 – točka 10

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(10) „evropski certifikat kibernetske varnosti“ pomeni dokument, ki ga izda organ za ugotavljanje skladnosti in potrjuje, da zadevni izdelek ali ***storitev*** IKT izpolnjuje posebne zahteve, določene v evropski certifikacijski shemi za kibernetsko varnost;	(10) „evropski certifikat kibernetske varnosti“ pomeni dokument, ki ga izda organ za ugotavljanje skladnosti in potrjuje, da zadevni izdelek***, storitev*** ali ***proces*** IKT izpolnjuje posebne zahteve, določene v evropski certifikacijski shemi za kibernetsko varnost;

Predlog spremembe 87

Predlog uredbe
Člen 2 – odstavek 1 – točka 11 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11a) „postopek IKT“ pomeni vrsto dejavnosti, ki se izvajajo za zasnovo, razvoj, vzdrževanje in dobavo izdelka ali storitve IKT;

Predlog spremembe 88

Predlog uredbe
Člen 2 – odstavek 1 – točka 11 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11b) „elektronska naprava za široko porabo“ pomenim napravo, sestavljeno iz strojne in programske opreme, ki obdeluje osebne podatke ali se povezuje z internetom za upravljanje domotike in aparatov za nadzor stanovanja, pisarniških aparatov ter naprav, ki se povezujejo v omrežje, kot so pametni televizijski sprejemniki, igrače in igralne konzole, virtualni ali osebni pomočniki, povezani predvajalniki, nosljive naprave, sistemi za glasovno upravljanje ter sistemi navidezne resničnosti;

Predlog spremembe 89

Predlog uredbe
Člen 2 – odstavek 1 – točka 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) ***„standard“*** pomeni standard, kot ***je opredeljen*** v ***točki*** (1) člena 2 Uredbe (EU) št. 1025/2012***.***	(16) ***„standard, tehnična specifikacija in tehnična specifikacija IKT“*** pomeni standard, ***tehnično specifikacijo ali tehnično specifikacijo IKT,*** kot ***so opredeljeni*** v ***točkah*** (1)***, (4) in (5)*** člena 2 Uredbe (EU) št. 1025/2012***;***

Predlog spremembe 90

Predlog uredbe
Člen 2 – odstavek 1 – točka 16 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(16a) „nacionalni organ za nadzor nad certificiranjem“ pomeni organ, ki ga posamezna država članica imenuje v skladu s členom 50 te uredbe;

Predlog spremembe 91

Predlog uredbe
Člen 2 – odstavek 1 – točka 16 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(16b) „samoocena“ pomeni izjavo o skladnosti, s katero proizvajalec izjavlja, da so bile izpolnjene določene zahteve iz certifikacijske sheme v zvezi s izdelki, postopki ali storitvami;

Predlog spremembe 92

Predlog uredbe
Člen 2 – odstavek 1 – točka 16 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(16c) „privzeta varnost“ pomeni situacijo, v kateri je mogoče izdelek, programsko opremo ali proces nastaviti tako, da zagotavlja višjo stopnjo varnosti, prvi uporabnik pa bi moral imeti privzeto konfiguracijo z najvarnejšimi možnimi nastavitvami. Če se na podlagi posameznega primera pri analizi tveganja ugotovi, da takšna nastavitev ni izvedljiva, bi bilo treba uporabnike spodbuditi, da se odločijo za najbolj varno nastavitev.

Predlog spremembe 93

Predlog uredbe
Člen 2 – odstavek 1 – točka 16 d (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(16d) „izvajalci bistvenih storitev“ pomeni izvajalce bistvenih storitev, kot so opredeljeni v točki (4) člena 4 Direktive (EU) 2016/1148;

Predlog spremembe 94

Predlog uredbe
Člen 3 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Agencija opravlja naloge, ki so ji dodeljene s to uredbo, in ***tako prispeva*** k ***visoki*** ravni kibernetske varnosti v Uniji.	1. Agencija opravlja naloge, ki so ji dodeljene s to uredbo, in ***se jo okrepi za namene prispevanja*** k ***doseganju visoke skupne*** ravni kibernetske varnosti***, da se preprečijo kibernetski napadi*** v Uniji***; da se zmanjša razdrobljenost notranjega trga in izboljša njegovo delovanje ter da se zagotovi skladnost, in sicer z upoštevanjem dosežkov držav članic pri sodelovanju v okviru direktive o varnosti omrežij in informacij***.

Predlog spremembe 95

Predlog uredbe
Člen 4 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Agencija je središče strokovnega znanja na področju kibernetske varnosti zaradi svoje neodvisnosti, znanstvene in tehnične kakovosti svetovanja, pomoči in informacij, ki jih zagotavlja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog.	1. Agencija je središče ***teoretičnega in praktičnega*** strokovnega znanja na področju kibernetske varnosti zaradi svoje neodvisnosti, znanstvene in tehnične kakovosti svetovanja, pomoči in informacij, ki jih zagotavlja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog.

Predlog spremembe 96

Predlog uredbe
Člen 4 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Agencija institucijam, agencijam in organom Unije ter državam članicam pomaga pri oblikovanju in izvajanju politik, ki se nanašajo na kibernetsko varnost.	2. Agencija institucijam, agencijam in organom Unije ter državam članicam pomaga pri oblikovanju in izvajanju politik, ki se nanašajo na kibernetsko varnost***, in pri ozaveščanju državljanov in podjetij***.

Predlog spremembe 97

Predlog uredbe
Člen 4 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Agencija podpira krepitev zmogljivosti in pripravljenost v ***celotni Uniji*** tako, da Uniji, državam članicam ter javnim in zasebnim zainteresiranim stranem pomaga krepiti zaščito njihovih omrežij in informacijskih sistemov, razvijati veščine, znanja in spretnosti na področju kibernetske varnosti ter doseči kibernetsko odpornost.	3. Agencija podpira krepitev zmogljivosti in pripravljenost v ***institucijah, agencijah in organih Unije*** tako, da Uniji, državam članicam ter javnim in zasebnim zainteresiranim stranem pomaga krepiti zaščito njihovih omrežij in informacijskih sistemov, razvijati ***in izboljševati kibernetsko odpornost in odzivne zmogljivosti, povečevati ozaveščenost in razvijati*** veščine, znanja in spretnosti na področju kibernetske varnosti ter doseči kibernetsko odpornost.

Predlog spremembe 98

Predlog uredbe
Člen 4 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Agencija pri zadevah, ki se nanašajo na kibernetsko varnost, spodbuja sodelovanje in ***usklajevanje*** na ravni Unije med državami članicami, institucijami, agencijami in organi Unije ter zadevnimi zainteresiranimi stranmi***, vključno z zasebnim sektorjem***.	4. Agencija pri zadevah, ki se nanašajo na kibernetsko varnost, spodbuja sodelovanje***, usklajevanje*** in ***izmenjavo informacij*** na ravni Unije med državami članicami, institucijami, agencijami in organi Unije ter zadevnimi zainteresiranimi stranmi.

Predlog spremembe 99

Predlog uredbe
Člen 4 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Agencija ***krepi*** zmogljivosti na področju kibernetske varnosti na ravni Unije, da bi dopolnila ukrepe držav članic pri preprečevanju kibernetskih groženj in odzivanju nanje, zlasti v primeru	5. Agencija ***prispeva h krepitvi*** zmogljivosti na področju kibernetske varnosti na ravni Unije, da bi dopolnila ukrepe držav članic pri preprečevanju kibernetskih groženj in odzivanju nanje,

čezmejnih incidentov.

zlasti v primeru čezmejnih incidentov***, ter da bi izvajala svojo nalogo zagotavljanja pomoči institucijam Unije pri oblikovanju politik, povezanih s kibernetsko varnostjo***.

Predlog spremembe 100

Predlog uredbe
Člen 4 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Agencija spodbuja uporabo certificiranja, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije v skladu z naslovom III te uredbe, in tako krepi preglednost zagotovil izdelkov in ***storitev*** IKT glede kibernetske varnosti kot tudi zaupanje v digitalni notranji trg.	6. Agencija spodbuja uporabo certificiranja, ***da bi se preprečila razdrobljenost notranjega trga in izboljšalo njegovo delovanje,*** vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije v skladu z naslovom III te uredbe, in tako krepi preglednost zagotovil izdelkov***, storitev*** in ***procesov*** IKT glede kibernetske varnosti kot tudi zaupanje v digitalni notranji trg ***ter povečuje skladnost med obstoječimi nacionalnimi in mednarodnimi certifikacijskimi shemami***.

Predlog spremembe 101

Predlog uredbe
Člen 4 – odstavek 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
7. Agencija spodbuja ***visoko raven*** ozaveščenosti državljanov in podjetij pri vprašanjih v zvezi s kibernetsko varnostjo.	7. Agencija spodbuja ***in podpira projekte, ki prispevajo k visoki ravni*** ozaveščenosti***, kibernetske higiene ter kibernetske pismenosti*** državljanov in podjetij pri vprašanjih v zvezi s kibernetsko varnostjo.

Predlog spremembe 102

Predlog uredbe
Člen 5 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. pomočjo in svetovanjem, zlasti z zagotavljanjem neodvisnega mnenja in pripravljalnega dela za razvoj in pregled politike in prava Unije na področju kibernetske varnosti ter panožne politike in pravnih pobud, kadar gre za zadeve, povezane s kibernetsko varnostjo;	1. pomočjo in svetovanjem, zlasti z zagotavljanjem neodvisnega mnenja***, analizo pomembnih dejavnosti v kibernetskem prostoru*** in ***zagotavljanjem*** pripravljalnega dela za razvoj in pregled politike in prava Unije na področju kibernetske varnosti ter panožne politike in pravnih pobud, kadar gre za zadeve, povezane s kibernetsko varnostjo;

Predlog spremembe 103

Predlog uredbe
Člen 5 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. pomočjo državam članicam pri doslednem izvajanju politike in prava Unije na področju kibernetske varnosti, zlasti v zvezi z Direktivo (EU) 2016/1148, vključno z mnenji, smernicami, svetovanjem in najboljšimi praksami na področjih, kot so obvladovanje tveganj, poročanje o incidentih in izmenjava informacij, ter lažjo izmenjavo najboljših praks med pristojnimi organi v tem oziru;	2. pomočjo državam članicam pri doslednem izvajanju politike in prava Unije na področju kibernetske varnosti, zlasti v zvezi z Direktivo (EU) 2016/1148, ***Direktivo ... o evropskem zakoniku o elektronskih komunikacijah, Uredbo (EU) 2016/679 in Direktivo 2002/58/ES,*** vključno z mnenji, smernicami, svetovanjem in najboljšimi praksami na področjih, kot so ***varna programska oprema in razvoj sistemov,*** obvladovanje tveganj, poročanje o incidentih in izmenjava informacij, ***tehnični in organizacijski ukrepi, zlasti vzpostavitev programov za usklajeno razkrivanje šibkih točk,*** ter lažjo izmenjavo najboljših praks med pristojnimi organi v tem oziru;

Predlog spremembe 104

Predlog uredbe
Člen 5 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. oblikovanjem in spodbujanjem politik, ki bi ohranjale splošno dostopnost

	oziroma celovitost javnega jedra odprtega interneta, ki zagotavlja ključno funkcionalnost interneta kot celote in je temeljnega pomena za njegovo normalno delovanje, med drugim varnost in stabilnost ključnih protokolov (zlasti DNS, BGP in IPv6), delovanje sistema domenskih imen (vključno z vsemi najvišjimi domenami) in delovanje korenske cone;

Predlog spremembe 105

Predlog uredbe
Člen 5 – odstavek 4 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) spodbujanju višje ravni varnosti elektronskih komunikacij, med drugim z zagotavljanjem strokovnega znanja in svetovanja, ter lažji izmenjavi najboljših praks med pristojnimi organi;	(2) spodbujanju višje ravni varnosti elektronskih komunikacij ***ter hrambe in obdelave podatkov***, med drugim z zagotavljanjem strokovnega znanja in svetovanja, ter lažji izmenjavi najboljših praks med pristojnimi organi;

Predlog spremembe 106

Predlog uredbe
Člen 5 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. pomoči državam članicam pri doslednem izvajanju politike in prava Unije v zvezi z varstvom podatkov, zlasti Uredbe (EU) 2016/679, ter pomoči Evropskemu odboru za varstvo podatkov pri oblikovanju smernic v zvezi z izvajanjem Uredbe (EU) 2016/679 za namene kibernetske varnosti. Evropski odbor za varstvo podatkov se z agencijo posvetuje vsakič, ko izda mnenje ali odločitev o izvajanju splošne uredbe o varstvu podatkov in kibernetske varnosti, neizčrpno pa glede vprašanj, povezanih z ocenami učinka na zasebnost, obveščanju o kršitvah podatkov, varnostno obdelavo,

varnostnih zahtevah ter vgrajeni zasebnosti.

Predlog spremembe 107

Predlog uredbe
Člen 6 – odstavek 1 – točka a a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) državam članicam in institucijam Unije pri vzpostavljanju in izvajanju politik za usklajeno razkrivanje šibkih točk ter procesov za pregled vladnega razkrivanja šibkih točk, pri čemer bi morale biti njihove prakse in odločitve pregledne in predmet neodvisnega nadzora.

Predlog spremembe 108

Predlog uredbe
Člen 6 – odstavek 1 – točka a b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ab) Agencija olajša vzpostavitev in začetek izvajanja dolgoročnega projekta evropske informacijske varnosti, da bi v sodelovanju z Evropskim raziskovalnim svetom (ERC) in Evropskim inštitutom za inovacije in tehnologijo (EIT) ter v skladu z raziskovalnimi programi Unije nadalje spodbujala raziskave kibernetske varnosti v Uniji in državah članicah.

Predlog spremembe 109

Predlog uredbe
Člen 6 – odstavek 1 – točka g

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(g) državam članicam z organiziranjem letnih obsežnih vaj na področju kibernetske varnosti na ravni Unije iz člena 7(6) in z	(g) državam članicam z organiziranjem ***rednih in vsaj*** letnih obsežnih vaj na področju kibernetske varnosti na ravni

oblikovanjem političnih priporočil, ki temeljijo na postopku ocenjevanja vaj in izkušnjah, pridobljenih z njimi;	Unije iz člena 7(6) in z oblikovanjem političnih priporočil ***in izmenjavanjem primerov najboljše prakse***, ki temeljijo na postopku ocenjevanja vaj in izkušnjah, pridobljenih z njimi;

Predlog spremembe 110

Predlog uredbe
Člen 6 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Agencija olajšuje vzpostavitev sektorskih centrov za izmenjavo in analizo informacij (ISAC) in jih stalno podpira, zlasti v sektorjih, ki so navedeni v Prilogi II k Direktivi (EU) 2016/1148, in sicer z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih in ***postopkih*** ter o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij.	2. Agencija olajšuje vzpostavitev sektorskih centrov za izmenjavo in analizo informacij (ISAC) in jih stalno podpira, zlasti v sektorjih, ki so navedeni v Prilogi II k Direktivi (EU) 2016/1148, in sicer z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih***, postopkih*** in ***načelih kibernetske higiene*** ter o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij.

Predlog spremembe 111

Predlog uredbe
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Agencija podpira operativno sodelovanje med ***pristojnimi javnimi organi*** in med zainteresiranimi stranmi.	1. Agencija podpira operativno sodelovanje med ***državami članicami, institucijami, agencijami*** in ***organi Unije ter*** med zainteresiranimi stranmi***, da bi z analizo in oceno obstoječih nacionalnih shem, oblikovanjem in izvajanjem načrta ter uporabo ustreznih instrumentov za doseganje najvišje ravni certificiranja kibernetske varnosti v Uniji in državah članicah vzpostavila medsebojno sodelovanje***.

Predlog spremembe 112

Predlog uredbe

Člen 7 – odstavek 4 – pododstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) zagotavljanjem, na njihovo zahtevo, tehnične pomoči ob incidentih, ki imajo pomembne ali znatne posledice;	(b) zagotavljanjem, na njihovo zahtevo, tehnične pomoči ***v obliki izmenjave informacij ter strokovnega znanja*** ob incidentih, ki imajo pomembne ali znatne posledice;

Predlog spremembe 113

Predlog uredbe
Člen 7 – odstavek 4 – pododstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) Če je treba v določenih razmerah, ko ima incident znatno moteč učinek, hitro ukrepati, lahko država članica pri oceni razmer zaprosi za pomoč strokovnjakov iz Agencije. Prošnja obsega opis razmer, morebitne namene in predvidene potrebe.

Predlog spremembe 114

Predlog uredbe
Člen 7 – odstavek 5 – pododstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Agencija na zahtevo ***dveh*** ali več zadevnih držav članic in z izključnim namenom zagotavljanja svetovanja za preprečevanje prihodnjih incidentov zagotovi podporo za naknadno tehnično preiskavo ali jo izvede, potem ko prizadeta podjetja priglasijo incidente, ki imajo pomembne ali znatne posledice v skladu z Direktivo (EU) 2016/1148. Agencija takšno preiskavo izvede tudi na ustrezno utemeljeno zahtevo Komisije in v soglasju z zadevnimi državami članicami v primeru incidentov, ki prizadenejo več kot ***dve državi članici***.	Agencija na zahtevo ***ene*** ali več zadevnih držav članic in z izključnim namenom zagotavljanja ***pomoči, in sicer v obliki*** svetovanja za preprečevanje prihodnjih incidentov ***ali v obliki pomoči pri odzivu na trenutne obsežne incidente,*** zagotovi podporo za naknadno tehnično preiskavo ali jo izvede, potem ko prizadeta podjetja priglasijo incidente, ki imajo pomembne ali znatne posledice v skladu z Direktivo (EU) 2016/1148. Agencija ***zgoraj navedene dejavnosti izvaja tako, da prejme ustrezne informacije od prizadetih držav članic in uporabi svoja sredstva za analizo nevarnosti in odziv na incidente. Agencija***

	takšno preiskavo izvede tudi na ustrezno utemeljeno zahtevo Komisije in v soglasju z zadevnimi državami članicami v primeru incidentov, ki prizadenejo več kot ***eno državo članico. Pri tem zagotovi, da ne razkrije ukrepov, ki so jih države članice sprejele za ohranitev njihovih temeljnih državnih funkcij, zlasti tistih, ki zadevajo nacionalno varnost***.

Predlog spremembe 115

Predlog uredbe
Člen 7 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Agencija organizira letne vaje na področju kibernetske varnosti na ravni Unije ter države članice in institucije, agencije in organe Unije podpira pri organiziranju vaj na podlagi njihovih zahtev. Letne vaje na ravni Unije vključujejo tehnične, operativne in strateške elemente ter pripomorejo k pripravi sodelovalnega odziva na ravni Unije na velike čezmejne kibernetske incidente. Poleg tega Agencija prispeva k sektorskim vajam na področju kibernetske varnosti in jih po potrebi pomaga organizirati skupaj z ustreznimi centri za izmenjavo in analizo informacij (ISAC) ter tem centrom omogoča, da sodelujejo pri vajah na področju kibernetske varnosti tudi na ravni Unije.	6. Agencija organizira ***redne, v vsakem primeru pa vsaj*** letne vaje na področju kibernetske varnosti na ravni Unije ter države članice in institucije, agencije in organe Unije podpira pri organiziranju vaj na podlagi njihovih zahtev. Letne vaje na ravni Unije vključujejo tehnične, operativne in strateške elemente ter pripomorejo k pripravi sodelovalnega odziva na ravni Unije na velike čezmejne kibernetske incidente. Poleg tega Agencija prispeva k sektorskim vajam na področju kibernetske varnosti in jih po potrebi pomaga organizirati skupaj z ustreznimi centri za izmenjavo in analizo informacij (ISAC) ter tem centrom omogoča, da sodelujejo pri vajah na področju kibernetske varnosti tudi na ravni Unije.

Predlog spremembe 116

Predlog uredbe
Člen 7 – odstavek 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
7. Agencija pripravi redno tehnično poročilo o incidentih in grožnjah na področju kibernetske varnosti v EU, in sicer na podlagi prosto dostopnih virov,	7. Agencija pripravi redno ***in poglobljeno*** tehnično poročilo o incidentih in grožnjah na področju kibernetske varnosti v EU, in sicer na podlagi prosto

lastne analize in poročil, ki jih predložijo med drugim: skupine CSIRT držav članic (na prostovoljni osnovi) ali enotne kontaktne točke v skladu z direktivo o varnosti omrežij in informacij (členom 14(5) direktive o varnosti omrežij in informacij); Evropski center za boj proti kibernetski kriminaliteti (EC3) pri Europolu, CERT-EU.	dostopnih virov, lastne analize in poročil, ki jih predložijo med drugim: skupine CSIRT držav članic (na prostovoljni osnovi) ali enotne kontaktne točke v skladu z direktivo o varnosti omrežij in informacij (členom 14(5) direktive o varnosti omrežij in informacij); Evropski center za boj proti kibernetski kriminaliteti (EC3) pri Europolu, CERT-EU. ***Izvršni direktor Evropskemu parlamentu predstavi javne ugotovitve, kadar je to ustrezno.***

Predlog spremembe 117

Predlog uredbe
Člen 7 – odstavek 7 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	7a. Agencija, kadar je to ustrezno in po predhodni odobritvi Komisije, prispeva k spletnemu sodelovanju s centrom odličnosti zveze NATO za sodelovanje pri kibernetski obrambi in akademijo zveze NATO za komuniciranje in obveščanje.

Predlog spremembe 118

Predlog uredbe
Člen 7 – odstavek 8 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) združevanjem poročil iz nacionalnih virov, da bi prispevala k skupnemu situacijskemu zavedanju;	(a) ***analiziranjem in*** združevanjem poročil iz nacionalnih virov, da bi prispevala k skupnemu situacijskemu zavedanju;

Predlog spremembe 119

Predlog uredbe
Člen 7 – odstavek 8 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) podpiranjem tehničnega	(c) podpiranjem tehničnega

obravnavanja incidenta ali krize, vključno z olajševanjem izmenjave tehničnih rešitev med državami članicami;	obravnavanja incidenta ali krize ***na podlagi lastnega neodvisnega znanja in sredstev***, vključno z olajševanjem ***prostovoljne*** izmenjave tehničnih rešitev med državami članicami;

Predlog spremembe 120

Predlog uredbe
Člen 7 – odstavek 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	8a. Agencija po potrebi organizira izmenjavo mnenj in pomaga organom držav članic pri usklajevanju njihovega odziva v skladu z načeloma subsidiarnosti in sorazmernosti.

Predlog spremembe 121

Predlog uredbe
Člen 7 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 7a
	Tehnične zmogljivosti agencije ENISA
	1. Za doseganje ciljev, opisanih v členu 7, agencija ENISA v skladu s svojim delovnim programom med drugim razvije naslednje tehnične zmogljivosti in veščine:
	(a) zmožnost zbiranja informacij o kibernetskih grožnjah iz odprtega vira in
	(b) zmožnost za uporabo tehnične opreme, orodij in strokovnega znanja na daljavo.
	2. Za namen zagotovitve tehničnih zmogljivosti iz odstavka 1 tega člena in razvoja ustreznih veščin agencija ENISA:
	(a) zagotovi, da postopki zaposlovanja sledijo potrebam po različnih tehničnih veščinah in
	(b) sodeluje s skupino EU za odzivanje na

	računalniške grožnje (CERT EU) in Europolom v skladu s členom 7(2) te uredbe.

Predlog spremembe 122

Predlog uredbe
Člen 8 – odstavek 1 – točka a – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju izdelkov in storitev IKT glede kibernetske varnosti, kot je določeno v naslovu III te uredbe, in sicer s:	(a) podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju izdelkov in storitev ***ter postopkov*** IKT glede kibernetske varnosti, kot je določeno v naslovu III te uredbe, in sicer s:

Predlog spremembe 123

Predlog uredbe
Člen 8 – odstavek 1 – točka a – točka -1 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(-1) stalnim določanjem standardov, tehničnih specifikacij in informacijskih tehničnih specifikacij;

Predlog spremembe 124

Predlog uredbe
Člen 8 – odstavek 1 – točka a – točka 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost za izdelke ***in*** storitve IKT v skladu s členom 44 te uredbe;	(1) pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost za izdelke***,*** storitve ***in postopke*** IKT v skladu s členom 44 te uredbe ***v sodelovanju z zainteresiranimi stranmi v industriji in organizacijami za standardizacijo v okviru formalnega, standardiziranega in preglednega postopka***;

Predlog spremembe 125

Predlog uredbe
Člen 8 – odstavek 1 – točka a – točka 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(1a) izvajanjem ocenjevanja postopkov za izdajanje evropskih certifikatov kibernetske varnosti, ki so jih določili organi za ugotavljanje skladnosti iz člena 51 te uredbe, v sodelovanju s certifikacijsko skupino držav članic v skladu s členom 53 te uredbe z namenom, da bi zagotovili enotno izvajanje te uredbe s strani organov za ugotavljanje skladnosti, ko izdajajo certifikate;

Predlog spremembe 126

Predlog uredbe
Člen 8 – odstavek 1 – točka a – točka 1 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(1b) izvajanjem neodvisnih rednih naknadnih pregledov skladnosti certificiranih izdelkov, postopkov in storitev IKT z evropskimi certifikacijskimi shemami za kibernetsko varnost;

Predlog spremembe 127

Predlog uredbe
Člen 8 – odstavek 1 – točka a – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) podporo Komisiji pri zagotavljanju sekretariata ***Evropski*** certifikacijski skupini ***za kibernetsko varnost*** v skladu s členom 53 te uredbe;	(2) podporo Komisiji pri zagotavljanju sekretariata certifikacijski skupini ***držav članic*** v skladu s členom 53 te uredbe;

Predlog spremembe 128

Predlog uredbe

Člen 8 – odstavek 1 – točka a – točka 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) pripravo in objavo smernic ter razvojem dobrih praks glede zahtev na področju kibernetske varnosti za izdelke in storitve IKT v sodelovanju z nacionalnimi organi za nadzor nad certificiranjem in predstavniki industrije;	(3) pripravo in objavo smernic ter razvojem dobrih praks***, tudi glede načel kibernetske higiene,*** glede zahtev na področju kibernetske varnosti za izdelke***, postopke*** in storitve IKT v sodelovanju z nacionalnimi organi za nadzor nad certificiranjem in predstavniki industrije ***v okviru formalnega, standardiziranega in preglednega postopka***;

Predlog spremembe 129

Predlog uredbe
Člen 8 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) olajšuje vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganj in varnost izdelkov in storitev IKT ter v sodelovanju z državami članicami pripravi nasvete in smernice za tehnična področja, povezana z varnostnimi zahtevami za izvajalce bistvenih storitev in ponudnike digitalnih storitev, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, v skladu s členom 19(2) Direktive (EU) 2016/1148;	(b) olajšuje vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganj in varnost izdelkov***, postopkov*** in storitev IKT ter v sodelovanju z državami članicami ***in industrijo*** pripravi nasvete in smernice za tehnična področja, povezana z varnostnimi zahtevami za izvajalce bistvenih storitev in ponudnike digitalnih storitev, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, v skladu s členom 19(2) Direktive (EU) 2016/1148***, ter izmenjevanje teh informacij med državami članicami***;

Predlog spremembe 130

Predlog uredbe
Člen 9 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) v sodelovanju s strokovnjaki iz organov držav članic zagotavlja nasvete, smernice in najboljše prakse za varnost omrežij in informacijskih sistemov, zlasti	(c) v sodelovanju s strokovnjaki iz organov držav članic ***in ustreznimi zainteresiranimi stranmi*** zagotavlja nasvete, smernice in najboljše prakse za

za varnost internetne infrastrukture in infrastruktur, ki podpirajo sektorje iz Priloge II k Direktivi (EU) 2016/1148;	varnost omrežij in informacijskih sistemov, zlasti za varnost internetne infrastrukture in infrastruktur, ki podpirajo sektorje iz Priloge II k Direktivi (EU) 2016/1148;

Predlog spremembe 131

Predlog uredbe
Člen 9 – odstavek 1 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) javnost ozavešča o tveganjih glede kibernetske varnosti ***in*** zagotavlja smernice o dobrih praksah za ***posamezne*** uporabnike, ki so namenjene državljanom in organizacijam;	(e) javnost ***redno*** ozavešča o tveganjih glede kibernetske varnosti***,*** zagotavlja ***usposabljanje in*** smernice o dobrih praksah za uporabnike, ki so namenjene državljanom in organizacijam***, ter spodbuja sprejetje strogih preventivnih ukrepov informacijske varnosti in zanesljivo varstvo podatkov in zasebnosti***;

Predlog spremembe 132

Predlog uredbe
Člen 9 – odstavek 1 – točka g

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(g) v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizira redne kampanje ***ozaveščanja*** za ***izboljšanje kibernetske varnosti in njene prepoznavnosti v Uniji***.	(g) v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizira redne ***komunikacijske*** kampanje za ***spodbujanje široke javne razprave;***

Predlog spremembe 133

Predlog uredbe
Člen 9 – odstavek 1 – točka g a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ga) spodbuja tesnejše sodelovanje in izmenjavo najboljše prakse med državami članicami v zvezi z izobraževanjem o kibernetski varnosti in pismenostjo glede

kibernetske varnosti, kibernetsko higieno in doseganjem večje ozaveščenosti o tem.

Predlog spremembe 134

Predlog uredbe
Člen 10 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) svetuje Uniji in državam članicam o potrebah po raziskavah in prednostnih nalogah na področju kibernetske varnosti, da bi omogočila učinkovito odzivanje na aktualna in nastajajoča tveganja in grožnje, vključno z upoštevanjem novih in nastajajočih informacijskih in komunikacijskih tehnologij, ter učinkovito uporabo tehnologij za preprečevanje tveganj;	(a) ***zagotavlja predhodna posvetovanja z ustreznimi skupinami uporabnikov in*** svetuje Uniji in državam članicam o potrebah po raziskavah in prednostnih nalogah na področju kibernetske varnosti***, varstva podatkov in zasebnosti***, da bi omogočila učinkovito odzivanje na aktualna in nastajajoča tveganja in grožnje, vključno z upoštevanjem novih in nastajajočih informacijskih in komunikacijskih tehnologij, ter učinkovito uporabo tehnologij za preprečevanje tveganj;

Predlog spremembe 135

Predlog uredbe
Člen 10 – odstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) naroči lastne raziskovalne dejavnosti na interesnih področjih, ki še niso zajeta v obstoječih raziskovalnih programih Unije, če se ugotovi jasna evropska dodana vrednost.

Predlog spremembe 136

Predlog uredbe
Člen 11 – odstavek 1 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) svetuje in daje podporo Komisiji v sodelovanju s certifikacijsko skupino

	držav članic, ustanovljeno na podlagi člena 53, pri zadevah, povezanih s sporazumi o vzajemnem priznavanju certifikatov kibernetske varnosti s tretjimi državami.

Predlog spremembe 137

Predlog uredbe
Člen 12 – odstavek 1 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) ***stalna*** skupina ***zainteresiranih strani***, ki izvaja naloge iz člena 20.	(d) ***svetovalna*** skupina ***agencije ENISA***, ki izvaja naloge iz člena 20.

Predlog spremembe 138

Predlog uredbe
Člen 14 – odstavek 1 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) oceni in sprejme konsolidirano letno poročilo o dejavnostih Agencije ter poročilo in njegovo oceno do 1. julija naslednjega leta pošlje Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču. Letno poročilo vključuje zaključni račun in ***opisuje***, kako je ***Agencija*** izpolnila svoje kazalnike uspešnosti. Letno poročilo se objavi;	(e) oceni in sprejme konsolidirano letno poročilo o dejavnostih agencije ***ENISA*** ter poročilo in njegovo oceno do 1. julija naslednjega leta pošlje Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču. Letno poročilo vključuje zaključni račun***, opis učinkovitosti odhodkov*** in ***oceno učinkovitosti Agencije ter tega***, kako je izpolnila svoje kazalnike uspešnosti. Letno poročilo se objavi;

Predlog spremembe 139

Predlog uredbe
Člen 14 – odstavek 1 – točka m

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(m) imenuje izvršnega direktorja in po potrebi podaljša njegov mandat ali ga razreši s položaja v skladu s členom 33 te uredbe;	(m) imenuje izvršnega direktorja***, izbranega na podlagi strokovnih meril,*** in po potrebi podaljša njegov mandat ali ga razreši s položaja v skladu s členom 33 te

uredbe;

Predlog spremembe 140

Predlog uredbe
Člen 14 – odstavek 1 – točka o

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
o) sprejme vse odločitve glede vzpostavitve notranjih struktur Agencije in po potrebi njihovih sprememb, pri čemer upošteva potrebe pri dejavnostih Agencije in dobro proračunsko upravljanje;	o) sprejme vse odločitve glede vzpostavitve notranjih struktur Agencije in po potrebi njihovih sprememb, pri čemer upošteva potrebe pri dejavnostih Agencije***, kot so navedene v tej uredbi,*** in dobro proračunsko upravljanje;

Predlog spremembe 141

Predlog uredbe
Člen 16 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Člani ***stalne skupine zainteresiranih strani*** lahko na povabilo predsednika sodelujejo na sejah upravnega odbora, vendar nimajo glasovalne pravice.	4. Člani ***svetovalna skupina agencije ENISA*** lahko na povabilo predsednika sodelujejo na sejah upravnega odbora, vendar nimajo glasovalne pravice.

Predlog spremembe 142

Predlog uredbe
Člen 18 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Izvršni odbor sestavlja pet članov, imenovanih izmed članov upravnega odbora, vključno s predsednikom upravnega odbora, ki lahko predseduje tudi izvršnemu odboru, eden od članov pa je predstavnik Komisije. Izvršni direktor se udeležuje sej izvršnega odbora, vendar nima glasovalne pravice.	3. Izvršni odbor sestavlja pet članov, imenovanih izmed članov upravnega odbora, vključno s predsednikom upravnega odbora, ki lahko predseduje tudi izvršnemu odboru, eden od članov pa je predstavnik Komisije. Izvršni direktor se udeležuje sej izvršnega odbora, vendar nima glasovalne pravice. ***Cilj pri postopku imenovanja je doseči uravnoteženo zastopanost spolov v izvršnem odboru.***

Obrazložitev

Pri imenovanju članov izvršnega odbora je prav tako cilj doseči uravnoteženo zastopanost spolov, pri čemer se je treba zgledovati po določbah za upravni odbor v členu 13(3).

Predlog spremembe 143

Predlog uredbe
Člen 19 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Izvršni direktor na zahtevo poroča Evropskemu parlamentu o opravljanju svojih dolžnosti. Svet lahko izvršnega direktorja pozove, naj poroča o opravljanju svojih dolžnosti.	2. Izvršni direktor ***letno ali*** na zahtevo poroča Evropskemu parlamentu o opravljanju svojih dolžnosti. Svet lahko izvršnega direktorja pozove, naj poroča o opravljanju svojih dolžnosti.

Predlog spremembe 144

Predlog uredbe
Člen 19 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. tudi izvršni direktor ima pravico, da deluje kot posebni svetovalec predsednika Evropske komisije za področje politike kibernetske varnosti institucij, z mandatom, opredeljenim v Odločbi Komisije C (2014) 541 z dne 6. februarja 2014.

Predlog spremembe 145

Predlog uredbe
Člen 20 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Stalna skupina ***zainteresiranih strani***	***Svetovalna*** skupina ***agencije ENISA***
	(Sprememba velja za celotno besedilo; če bo sprejeta, bodo potrebne ustrezne prilagoditve v celotnem besedilu.)

Predlog spremembe 146

Predlog uredbe
Člen 20 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Na predlog izvršnega direktorja upravni odbor ustanovi ***stalno*** skupino ***zainteresiranih strani***, ki jo sestavljajo priznani strokovnjaki, ki zastopajo ustrezne zainteresirane strani, kot so podjetja iz sektorja IKT, ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, skupine potrošnikov, znanstveniki s področja kibernetske varnosti in predstavniki pristojnih organov, ki so uradno obveščeni v skladu z [direktivo o evropskem zakoniku o elektronskih komunikacijah], ter organi pregona in nadzorni organi za varstvo podatkov.	1. Na predlog izvršnega direktorja upravni odbor ***na pregleden način*** ustanovi ***svetovalno*** skupino ***agencije ENISA***, ki jo sestavljajo priznani strokovnjaki ***za varnost***, ki zastopajo ustrezne zainteresirane strani, kot so podjetja iz sektorja IKT, ***vključno z malimi in srednjimi podjetji, izvajalci bistvenih storitev v skladu z direktivo o varnosti omrežij in informacij,*** ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, skupine potrošnikov, znanstveniki s področja kibernetske varnosti***, evropske organizacije za standardizacijo, agencije EU*** in predstavniki pristojnih organov, ki so uradno obveščeni v skladu z [direktivo o evropskem zakoniku o elektronskih komunikacijah], ter organi pregona in nadzorni organi za varstvo podatkov. ***Upravni odbor zagotovi ustrezno ravnotežje med različnimi skupinami zainteresiranih strani.***

Predlog spremembe 147

Predlog uredbe
Člen 20 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Postopki ***stalne*** skupine ***zainteresiranih strani***, ki se nanašajo predvsem na število, sestavo, imenovanje članov s strani upravnega odbora, predlog s strani izvršnega direktorja in delovanje skupine, se določijo v statutu Agencije in objavijo.	2. Postopki ***svetovalne*** skupine ***agencije ENISA***, ki se nanašajo predvsem na število, sestavo, imenovanje članov s strani upravnega odbora, predlog s strani izvršnega direktorja in delovanje skupine, se določijo v statutu Agencije in objavijo.

Predlog spremembe 148

Predlog uredbe
Člen 20 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. ***Stalni*** skupini ***zainteresiranih strani*** predseduje izvršni direktor ali katera koli oseba, ki jo izvršni direktor imenuje za vsak primer posebej.	3. ***Svetovalni*** skupini ***agencije ENISA*** predseduje izvršni direktor ali katera koli oseba, ki jo izvršni direktor imenuje za vsak primer posebej.

Predlog spremembe 149

Predlog uredbe
Člen 20 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Mandat članov ***stalne*** skupine ***zainteresiranih strani*** traja dve leti in pol. Člani upravnega odbora ne smejo biti člani ***stalne*** skupine ***zainteresiranih strani***. Strokovnjaki iz Komisije in držav članic imajo pravico biti prisotni na sejah ***stalne*** skupine ***zainteresiranih strani*** in sodelovati pri njenem delu. Na seje in k sodelovanju pri delu skupine so lahko povabljeni predstavniki drugih organov, ki niso člani ***stalne*** skupine ***zainteresiranih strani***, za katere izvršni direktor meni, da so relevantni.	4. Mandat članov ***svetovalne*** skupine ***agencije ENISA*** traja dve leti in pol. Člani upravnega odbora ne smejo biti člani ***svetovalne*** skupine ***agencije ENISA***. Strokovnjaki iz Komisije in držav članic imajo pravico biti prisotni na sejah ***svetovalne*** skupine ***agencije ENISA*** in sodelovati pri njenem delu. Na seje in k sodelovanju pri delu skupine so lahko povabljeni predstavniki drugih organov, ki niso člani ***svetovalne*** skupine ***agencije ENISA***, za katere izvršni direktor meni, da so relevantni.

Predlog spremembe 150

Predlog uredbe
Člen 20 – odstavek 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4a. Svetovalna skupina agencije ENISA bo vse leto redno posodabljala svoje načrte, svoje cilje pa navedla v delovnem programu, ki bo zaradi preglednosti objavljen vsakih šest mesecev;

Predlog spremembe 151

Predlog uredbe
Člen 20 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. ***Stalna*** skupina ***zainteresiranih strani*** Agenciji svetuje glede opravljanja dejavnosti. Zlasti svetuje izvršnemu direktorju pri pripravi predloga delovnega programa Agencije in komuniciranju z ustreznimi zainteresiranimi stranmi o zadevah, ki se nanašajo na delovni program.	5. ***Svetovalna*** skupina ***agencije ENISA*** Agenciji svetuje glede opravljanja dejavnosti***, razen glede uporabe Naslova III te uredbe***. Zlasti svetuje izvršnemu direktorju pri pripravi predloga delovnega programa Agencije in komuniciranju z ustreznimi zainteresiranimi stranmi o zadevah, ki se nanašajo na delovni program.

Predlog spremembe 152

Predlog uredbe
Člen 20 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 20a
	Skupina zainteresiranih strani za certificiranje
	1. Izvršni direktor ustanovi skupino zainteresiranih strani za certificiranje, ki jo sestavlja splošni svetovalni odbor, katerega naloga je zagotavljati splošne nasvete o uporabi naslova III te uredbe, ter posebne odbore, ki predlagajo, razvijajo in sprejemajo posamezne predloge za shemo. Člani skupine se izberejo izmed priznanih strokovnjakov za varnost, ki zastopajo ustrezne zainteresirane strani, kot so podjetja iz sektorja IKT, vključno z malimi in srednjimi podjetji, izvajalci bistvenih storitev v skladu z direktivo o varnosti omrežij in informacij, ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, skupine potrošnikov, znanstveniki s področja kibernetske varnosti, evropske organizacije za standardizacijo, predstavniki pristojnih organov, ki so uradno obveščeni v skladu z [direktivo o evropskem zakoniku o elektronskih

	komunikacijah], ter organi pregona in nadzorni organi za varstvo podatkov.
	2. Postopki skupine zainteresiranih strani za certificiranje, ki se nanašajo predvsem na število, sestavo in imenovanje članov s strani izvršnega direktorja, se določijo v statutu agencije ENISA in objavijo, pri zagotavljanju pravične zastopanosti in enakih pravic za vse zainteresirane strani pa sledijo najboljši praksi.
	3. Člani upravnega odbora ne smejo biti člani skupine zainteresiranih strani za certificiranje. Člani svetovalne skupine agencije ENISA so lahko tudi člani skupine zainteresiranih strani za certificiranje. Strokovnjaki iz Komisije in držav članic imajo pravico, da na povabilo sodelujejo na sejah skupine zainteresiranih strani za certificiranje. Na seje in k sodelovanju pri delu skupine zainteresiranih strani za certificiranje se lahko povabijo predstavniki drugih organov, ki so po mnenju izvršnega direktorja ustrezni.
	4. Skupina zainteresiranih strani za certificiranje agenciji ENISA svetuje glede opravljanja dejavnosti v zvezi z Naslovom III te uredbe. Skupina je zlasti upravičena, da Komisiji predlaga pripravo predloge za evropske certifikacijske sheme za kibernetsko varnost, kot je določeno v členu 44 te uredbe, ter da sodeluje pri postopkih za odobritev takih shem iz členov 43 do 48 in člena 53 uredbe.

Predlog spremembe 153

Predlog uredbe
Člen 21 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 21a
	Zahteve, naslovljene na agencijo ENISA
	1. Agencija ENISA bi morala vzpostaviti

	in upravljati enotno vstopno točko, prek katere se obravnavajo zahteve po svetovanju in pomoči, ki spadajo v njene cilje in naloge. Zahtevam morajo biti priložene osnovne informacije za pojasnitev vprašanja, ki ga je treba obravnavati. Agencija bi morala pripraviti opis morebitnih posledic za vire ter se pravočasno odzvati na zahteve. Če Agencija zahtevo zavrne, to obrazloži.
	2. Zahteve iz prvega odstavka lahko vložijo:
	a) Evropski parlament;
	b) Svet;
	c) Komisija in
	d) vsi pristojni organi, ki jih imenuje država članica, npr. nacionalni regulativni organi, kot so določeni v členu 2 Direktive 2002/21/ES.
	3. Upravni odbor v statutu agencije ENISA navede praktične podrobnosti glede uporabe odstavka 1 in 2, zlasti glede vložitve, določitve prednosti, nadaljnjih ukrepov ter obveščanja.

Predlog spremembe 154

Predlog uredbe
Člen 24 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Člani upravnega odbora, izvršni direktor, člani ***stalne*** skupine ***zainteresiranih strani***, zunanji strokovnjaki, ki sodelujejo v ad hoc delovnih skupinah, in osebje Agencije, tudi iz držav članic začasno napoteni uradniki, upoštevajo zahteve glede zaupnosti v skladu s členom 339 Pogodbe o delovanju Evropske unije (PDEU) tudi po prenehanju svojih dolžnosti.	2. Člani upravnega odbora, izvršni direktor, člani ***svetovalne*** skupine ***agencije ENISA***, zunanji strokovnjaki, ki sodelujejo v ad hoc delovnih skupinah, in osebje Agencije, tudi iz držav članic začasno napoteni uradniki, upoštevajo zahteve glede zaupnosti v skladu s členom 339 Pogodbe o delovanju Evropske unije (PDEU) tudi po prenehanju svojih dolžnosti.

Predlog spremembe 155

Predlog uredbe
Člen 26 – odstavek 1 – pododstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Začasen osnutek poročila o oceni temelji na ciljih in pričakovanih rezultatih iz enotnega programskega dokumenta iz člena 21(1) te uredbe ter v skladu z načelom oblikovanja proračuna glede na uspešnost upošteva finančne vire, ki so potrebni za dosego teh ciljev in pričakovanih rezultatov.

Predlog spremembe 156

Predlog uredbe
Člen 30 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Računsko sodišče lahko opravi revizije na podlagi dokumentacije in na kraju samem pri vseh upravičencih do nepovratnih sredstev, izvajalcih in podizvajalcih, ki so prejeli sredstva Unije od Agencije.	2. Računsko sodišče lahko opravi revizije na podlagi dokumentacije in ***pregledov*** na kraju samem pri vseh upravičencih do nepovratnih sredstev, izvajalcih in podizvajalcih, ki so prejeli sredstva Unije od Agencije.

Predlog spremembe 157

Predlog uredbe
Člen 36 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Osebno odgovornost uslužbencev do Agencije urejajo ustrezni pogoji, ki veljajo za osebje Agencije.	5. Osebno odgovornost uslužbencev do Agencije urejajo ustrezni pogoji, ki veljajo za osebje Agencije. ***Zagotovi se učinkovito zaposlovanje osebja.***

Predlog spremembe 158

Predlog uredbe
Člen 37 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Prevajalske storitve, potrebne za delovanje Agencije, ***zagotavlja*** Prevajalski center za organe Evropske unije.	2. Prevajalske storitve, potrebne za delovanje Agencije, ***zagotavljajo*** Prevajalski center za organe Evropske unije ***ali drugi ponudniki prevajalskih storitev v skladu s pravili o javnem naročanju in v mejah, določenih z ustreznimi finančnimi pravili***.

Predlog spremembe 159

Predlog uredbe
Člen 39 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Agencija lahko sodeluje s pristojnimi organi tretjih držav ali mednarodnimi organizacijami ali obojimi, kolikor je to potrebno za dosego ciljev iz te uredbe. V ta namen lahko Agencija na podlagi predhodne odobritve Komisije vzpostavi delovne dogovore z organi tretjih držav in mednarodnimi organizacijami. Ti dogovori ne ustvarjajo novih pravnih obveznosti za Unijo in njene države članice.	1. Agencija lahko sodeluje s pristojnimi organi tretjih držav ali mednarodnimi organizacijami ali obojimi, kolikor je to potrebno za dosego ciljev iz te uredbe. V ta namen lahko Agencija na podlagi predhodne odobritve Komisije vzpostavi delovne dogovore z organi tretjih držav in mednarodnimi organizacijami. ***Sodelovanje z zvezo NATO, kjer poteka, lahko vključuje skupne vaje na področju kibernetske varnosti in skupno usklajevanje odzivanja na kibernetske incidente.*** Ti dogovori ne ustvarjajo novih pravnih obveznosti za Unijo in njene države članice.

Obrazložitev

Zaradi čezmejne narave kibernetskih incidentov bi morala ENISA delovati skupaj s akterji kibernetske varnosti v Evropi, kot je zveza NATO, kjer je to primerno. To je še zlasti pomembno, ker ima lahko NATO kibernetske zmogljivosti, ki jih agencija ENISA nima, in obratno. V okviru večjih kibernetskih napadov, usmerjenih proti državam kot celoti, je za varnost Evrope nujno, da agencija ENISA sodeluje z mednarodnimi organizacijami, kot je NATO, na mednarodni ravni.

Predlog spremembe 160

Predlog uredbe
Člen 41 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Država članica, ki je gostiteljica Agencije, zagotovi optimalne pogoje za uspešno delovanje Agencije, vključno z dostopnostjo lokacije, ustreznimi šolami za otroke uslužbencev ter ustreznim dostopom do trga dela, socialne varnosti in zdravstvenega varstva za otroke in zakonce.	2. Država članica, ki je gostiteljica Agencije, zagotovi optimalne pogoje za uspešno delovanje Agencije, vključno z ***eno lokacijo za celotno Agencijo,*** dostopnostjo lokacije, ustreznimi šolami za otroke uslužbencev ter ustreznim dostopom do trga dela, socialne varnosti in zdravstvenega varstva za otroke in zakonce.

Obrazložitev

Sedanja struktura agencije ENISA z upravnim sedežem v Heraklionu in temeljnimi operacijami v Atenah se je izkazala za neučinkovito in drago. Vse osebje agencije ENISA bi zato moralo delati v istem mestu. Glede na merila iz tega odstavka bi morala agencija biti v Atenah.

Predlog spremembe 161

Predlog uredbe
Člen 43 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Evropska certifikacijska shema za kibernetsko varnost dokazuje, da izdelki in storitve IKT, ki so ***bili certificirani*** v ***skladu s tako shemo,*** izpolnjujejo določene zahteve glede njihove zmožnosti za odpornost, na določeni stopnji zagotovila, na ukrepe, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ponujajo ali so dostopni prek teh izdelkov, postopkov***,*** storitev in ***sistemov***.	Evropska certifikacijska shema za kibernetsko varnost dokazuje, da izdelki***, postopki*** in storitve IKT, ki so ***zajeti s to shemo,*** v ***času certifikacije nimajo znanih šibkih točk in*** izpolnjujejo določene zahteve***, ki se lahko nanašajo na evropske in mednarodne standarde, tehnične specifikacije in informacijske tehnične specifikacije*** glede njihove zmožnosti za odpornost***, v celotnem življenjskem ciklu***, na določeni stopnji zagotovila, na ukrepe, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ponujajo ali so dostopni prek teh izdelkov, postopkov ***in*** storitev***,*** in ***izpolnjujejo navedene varnostne cilje***.

Predlog spremembe 162

Predlog uredbe

Člen 44 – odstavek -1 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	-1. Komisija v skladu s členom 55a sprejme delegirane akte, ki to uredbo dopolnjujejo z vzpostavitvijo tekočega delovnega programa Unije za evropske certifikacijske sheme za kibernetsko varnost. V teh delegiranih aktih se opredelijo skupni ukrepi, ki jih je treba sprejeti na ravni Unije, ter strateške prednostne naloge. Tekoči delovni program Unije zlasti vsebuje prednostni seznam izdelkov, postopkov in storitev IKT, ki so primerni, da postanejo predmet evropske certifikacijske sheme za kibernetsko varnost, pa tudi analizo tega, ali med organi za ugotavljanje skladnosti in nacionalnimi organi za nadzor nad certificiranjem obstaja enakovredna raven kakovosti, tehničnega znanja in izkušenj in strokovnega znanja in, če je potrebno, predlog za ukrepe o tem, kako to doseči.
	Začetni tekoči delovni program Unije se določi najpozneje do... [šest mesecev po začetku veljavnosti te uredbe] in se po potrebi posodablja, v vsakem primeru pa vsaj vsaki dve leti. Tekoči delovni program se objavi.
	Pred sprejetjem ali posodobitvijo tekočega delovnega programa Unije se Komisija posvetuje s certifikacijsko skupino držav članic, agencijo ENISA in skupino zainteresiranih strani za certificiranje v okviru odprtega, preglednega in vključujočega posvetovanja.

Predlog spremembe 163

Predlog uredbe
Člen 44 – odstavek -1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	-1a. Komisija lahko v upravičenih primerih od agencije ENISA zahteva, naj pripravi predlogo za evropsko

	certifikacijsko shemo za kibernetsko varnost. Zahteva temelji na tekočem delovnem programu Unije.

Predlog spremembe 164

Predlog uredbe
Člen 44 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. ***Agencija ENISA na zahtevo Komisije pripravi predlogo*** za evropsko certifikacijsko shemo za kibernetsko varnost***, ki izpolnjuje zahteve*** iz ***členov*** 45, ***46 in*** 47 ***te uredbe. Države članice ali Evropska skupina*** za ***kibernetsko varnost (v nadaljnjem besedilu: skupina), ustanovljena v skladu s členom 53***, ***lahko Komisiji predlaga pripravo predloge za evropsko certifikacijsko shemo*** za ***kibernetsko varnost.***	1. ***Zahteva*** za evropsko certifikacijsko shemo za kibernetsko varnost ***vsebuje področje uporabe, varnostne cilje*** iz ***člena*** 45, ***ki se uporabljajo, elemente iz člena*** 47***, ki se uporabljajo, ter rok, do katerega mora posamezna predloga*** za ***shemo postati veljavna. Pri pripravi zahteve se Komisija lahko posvetuje z agencijo ENISA***, ***certifikacijsko skupino držav članic in skupino zainteresiranih strani*** za ***certificiranje.***

Predlog spremembe 165

Predlog uredbe
Člen 44 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Pri pripravi predlog za sheme iz odstavka 1 ***tega člena*** se agencija ENISA posvetuje z vsemi ustreznimi zainteresiranimi stranmi in tesno sodeluje s skupino. ***Skupina*** agenciji ENISA ***zagotavlja*** pomoč in strokovno svetovanje, ki ju agencija ENISA potrebuje pri pripravi predloge za shemo, vključno s pripravo mnenj, kadar je to potrebno.	2. Pri pripravi predlog za sheme iz odstavka **-**1 ***(novo)*** se agencija ENISA posvetuje z vsemi ustreznimi zainteresiranimi stranmi ***v okviru formalnega, odprtega, preglednega*** in ***vključujočega posvetovanja ter*** tesno sodeluje s ***certifikacijsko*** skupino ***držav članic, skupino zainteresiranih strani za certificiranje, posebnimi odbori v skladu s členom 20a te uredbe ter z evropskimi organi za standardizacijo***. ***Ti*** agenciji ENISA ***zagotovijo*** pomoč in strokovno svetovanje, ki ju agencija ENISA potrebuje pri pripravi predloge za shemo, vključno s pripravo mnenj, kadar je to potrebno.

Predlog spremembe 166

Predlog uredbe
Člen 44 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Agencija ENISA predlogo za ***evropsko certifikacijsko*** shemo ***za kibernetsko varnost***, pripravljeno v skladu z ***odstavkom*** 2 tega člena, pošlje Komisiji.	3. Agencija ENISA predlogo za shemo, pripravljeno v skladu z ***odstavkoma 1 in*** 2 tega člena, pošlje Komisiji.

Predlog spremembe 167

Predlog uredbe
Člen 44 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Komisija lahko na podlagi predloge za shemo, ki jo predlaga agencija ENISA, sprejme ***izvedbene*** akte v skladu s členom 55***(1), ki določajo evropske certifikacijske sheme*** za kibernetsko varnost za izdelke in storitve IKT, ki izpolnjujejo zahteve iz členov 45, 46 in 47 ***te uredbe***.	4. Komisija lahko na podlagi predloge za shemo, ki jo predlaga agencija ENISA, sprejme ***delegirane*** akte v skladu s členom 55***a za dopolnitev te uredbe z določitvijo evropskih certifikacijskih shem*** za kibernetsko varnost za izdelke***, postopke*** in storitve IKT, ki izpolnjujejo zahteve iz členov 45, 46 in 47.

Predlog spremembe 168

Predlog uredbe
Člen 44 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Agencija ENISA vzdržuje posebno spletišče, namenjeno obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost.	5. Agencija ENISA vzdržuje posebno spletišče, namenjeno obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost***, vključno z umaknjenimi in poteklimi certifikati, ter certifikati, ki jih zajema nacionalna certifikacija***. ***Če evropska certifikacijska shema za kibernetsko varnost izpolnjuje zahteve, ki naj bi jih skladno z ustrezno harmonizacijsko zakonodajo Unije izpolnjevala, Komisija nemudoma objavi***

	sklic na shemo v Uradnem listu Evropske unije ali v drugih sredstvih v skladu s pogoji, ki so določeni v ustreznem aktu harmonizacijske zakonodaje Unije.

Predlog spremembe 169

Predlog uredbe
Člen 44 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Agencija ENISA v skladu s strukturo, vzpostavljeno s to uredbo, pregleda sprejete sheme ob koncu njihove veljavnosti v skladu s členom 47 (1.ac) ali na zahtevo Komisije, pri čemer upošteva povratne informacije ustreznih zainteresiranih strani.

Predlog spremembe 170

Predlog uredbe
Člen 45 – odstavek 1 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Evropska certifikacijska shema za kibernetsko varnost je oblikovana tako, da ***ustrezno*** upošteva ***naslednje*** varnostne cilje:	Evropska certifikacijska shema za kibernetsko varnost je oblikovana tako, da upošteva varnostne cilje***, s katerimi se zagotovi***:

Predlog spremembe 171

Predlog uredbe
Člen 45 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ***zaščititi shranjene***, ***prenesene ali kako drugače obdelane podatke pred naključno ali nepooblaščeno hrambo, obdelavo***, ***dostopom ali razkritjem***;	(a) ***zaupnost***, ***celovitost, razpoložljivost in zasebnost storitev***, ***funkcij in podatkov***;

Predlog spremembe 172

Predlog uredbe
Člen 45 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) ***zaščititi shranjene***, ***prenesene ali kako drugače obdelane podatke pred naključnim ali nepooblaščenim uničenjem, naključno izgubo ali spremembo***;	(b) ***da do storitev***, ***funkcij in podatkov dostopajo in jih lahko uporabljajo le pooblaščene osebe in/ali pooblaščeni sistemi in programi***;

Predlog spremembe 173

Predlog uredbe
Člen 45 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) ***zagotoviti, da imajo pooblaščene osebe, programi ali stroji dostop izključno do podatkov, storitev ali funkcij***, ***na katere se nanašajo njihove pravice do dostopa***;	(c) ***da je vzpostavljen postopek za identifikacijo in evidentiranje vseh odvisnosti in znanih šibkih točk izdelkov***, ***postopkov in storitev IKT***;

Predlog spremembe 174

Predlog uredbe
Člen 45 – odstavek 1 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) ***beležiti, kateri podatki***, ***funkcije ali*** storitve ***so bili sporočeni, kdaj in kdo jih je sporočil***;	(d) ***da izdelki***, ***postopki in*** storitve ***IKT ne vsebujejo znanih šibkih točk***;

Predlog spremembe 175

Predlog uredbe
Člen 45 – odstavek 1 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) ***zagotoviti, da*** je ***mogoče preveriti, do katerih podatkov, storitev ali funkcij se je dostopalo ali kateri podatki***, ***storitve ali funkcije so se uporabljali ter kdaj*** in ***kdo je do njih dostopal oz. jih je uporabljal***;	(e) ***da*** je ***vzpostavljen postopek za obravnavanje na novo odkritih šibkih točk izdelkov***, ***postopkov*** in ***storitev IKT***;

Predlog spremembe 176

Predlog uredbe
Člen 45 – odstavek 1 – točka f

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(f) ***v primeru fizičnega ali tehničnega incidenta pravočasno povrniti razpoložljivost in dostop do podatkov, storitev*** in ***funkcij***;	(f) ***da so izdelki in storitve IKT razviti v skladu z načelom privzete*** in ***vgrajene varnosti***;

Predlog spremembe 177

Predlog uredbe
Člen 45 – odstavek 1 – točka g

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(g) ***zagotoviti,*** da so izdelki in storitve IKT opremljeni s posodobljeno programsko opremo, ki ne vsebuje znanih šibkih točk, in da so na voljo mehanizmi, ki zagotavljajo varno posodabljanje programske opreme.	(g) da so izdelki in storitve IKT opremljeni s posodobljeno programsko opremo, ki ne vsebuje znanih šibkih točk, in da so na voljo mehanizmi, ki zagotavljajo varno posodabljanje programske opreme.

Predlog spremembe 178

Predlog uredbe
Člen 45 – odstavek 1 – točka g a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ga) da so druga tveganja, povezana s kibernetskimi incidenti, kot so tveganja za življenje, zdravje, okolje in druge pomembne pravne interese, čim manjša.

Predlog spremembe 179

Predlog uredbe
Člen 46 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih stopenj zagotovila: osnovno, znatno in/ali visoko stopnjo zagotovila za izdelke in storitve IKT v shemi.	1. Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih stopenj zagotovila***, ki temeljijo na tveganju, v skladu z okoliščinami in predvideno uporabo izdelkov, postopkov in storitev IKT***: osnovno, znatno in/ali visoko stopnjo zagotovila za izdelke***, postopke*** in storitve IKT v shemi.

Predlog spremembe 180

Predlog uredbe
Člen 46 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) osnovna stopnja zagotovila ***se nanaša na certifikat, izdan*** v ***evropski certifikacijski shemi za kibernetsko varnost***, ***ki zagotavlja omejeno stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve*** IKT ***v zvezi s kibernetsko varnostjo,*** in ***je opredeljena s sklici na zadevne tehnične specifikacije, standarde in postopke***, ***vključno s tehničnim nadzorom, katerih namen je zmanjšati tveganje kibernetskih incidentov***;	(a) osnovna stopnja zagotovila ***ustreza nizkemu tveganju*** v ***smislu skupne verjetnosti in škode***, ***povezane z izdelkom, postopkom in storitvijo*** IKT***, ob upoštevanju predvidene uporabe*** in ***okoliščin. Osnovna stopnja zagotovila daje zaupanje***, ***da se je znanim osnovnim tveganjem kibernetskih nesreč mogoče zoperstaviti***;

Predlog spremembe 181

Predlog uredbe
Člen 46 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) znatna stopnja zagotovila ***se nanaša na certifikat, izdan*** v ***evropski certifikacijski shemi za kibernetsko varnost***, ***ki zagotavlja znatno stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve*** IKT ***v zvezi s kibernetsko varnostjo***, ***in*** je ***opredeljena s***	(b) znatna stopnja zagotovila ***ustreza višjemu tveganju*** v ***smislu skupne verjetnosti in škode***, ***povezane z izdelkom, postopkom in storitvijo*** IKT***. Znatna stopnja zagotovila daje zaupanje***, ***da*** je ***znana tveganja kibernetskih nesreč mogoče preprečiti*** in ***da je na voljo tudi***

sklici na zadevne tehnične specifikacije, standarde in ***postopke, vključno s tehničnim nadzorom, katerih namen je bistveno zmanjšati tveganje kibernetskih incidentov***;	***zmogljivost premagovanja kibernetskih napadov z omejenimi viri***;

Predlog spremembe 182

Predlog uredbe
Člen 46 – odstavek 2 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) visoka stopnja zagotovila ***se nanaša na certifikat, izdan*** v ***evropski certifikacijski shemi za kibernetsko varnost***, ***ki zagotavlja višjo stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve*** IKT ***v zvezi s kibernetsko varnostjo***, ***kot jo imajo certifikati z znatno stopnjo zagotovila, in*** je ***opredeljena s sklici na zadevne tehnične specifikacije, standarde*** in ***postopke, vključno s tehničnim nadzorom, katerih namen je preprečiti kibernetske incidente.***	(c) visoka stopnja zagotovila ***ustreza višjemu tveganju*** v ***smislu skupne verjetnosti in škode***, ***povezane z izdelkom, postopkom in storitvijo*** IKT***. Znatna stopnja zagotovila daje zaupanje***, ***da*** je ***tveganja kibernetskih nesreč mogoče preprečiti*** in ***da je na voljo tudi zmogljivost premagovanja najsodobnejšim kibernetskim napadom z znatnimi viri;***

Predlog spremembe 183

Predlog uredbe
Člen 46 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 46a
	Ocena stopenj zagotovila evropskih certifikacijskih shem za kibernetsko varnost
	1. Za osnovno raven zanesljivosti lahko proizvajalec ali ponudnik izdelkov, postopkov in storitev IKT opravi samooceno skladnosti, za katero je sam v celoti odgovoren.
	2. Za znatno raven zanesljivosti zagotovila ocena je vodilo pri ocenjevanju najmanj preverjanje skladnosti varnostnih

funkcionalnosti izdelka, postopka ali storitve z njegovo tehnično dokumentacijo;

3. Za visoko raven zanesljivosti je vodilo pri metodologiji ocenjevanja vsaj preskušanje učinkovitosti, pri katerem se ocenjuje odpornost varnostnih funkcionalnosti proti napadalcem, ki razpolagajo z znatnimi sredstvi.

Predlog spremembe 184

Predlog uredbe
Člen 47 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) predmet urejanja in področje uporabe certificiranja, vključno z vrsto ali kategorijami zajetih izdelkov in storitev IKT;	(a) predmet urejanja in področje uporabe certificiranja, vključno z vrsto ali kategorijami zajetih izdelkov***, postopkov*** in storitev IKT;

Predlog spremembe 185

Predlog uredbe
Člen 47 – odstavek 1 – točka a a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) področje uporabe in zahteve glede kibernetske varnosti, po potrebi pa tudi, da področje uporabe in navedene zahteve ustrezajo tistim v nacionalnih certifikatih o kibernetski varnosti, ki jih shema nadomešča ali so določene v pravnih aktih;

Predlog spremembe 186

Predlog uredbe
Člen 47 – odstavek 1 – točka a b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ab) obdobje veljavnosti certifikacijske

sheme;

Predlog spremembe 187

Predlog uredbe
Člen 47 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) podrobno specifikacijo zahtev glede kibernetske varnosti, glede na katere se ocenijo posamezni izdelki in storitve IKT, na primer s sklicem na ***standarde Unije*** ali mednarodne standarde ali tehnične specifikacije;	(b) podrobno specifikacijo zahtev glede kibernetske varnosti, glede na katere se ocenijo posamezni izdelki***, postopki*** in storitve IKT, na primer s sklicem na ***evropske*** ali mednarodne standarde***, tehnične specifikacije*** ali ***informacijske*** tehnične specifikacije***, ki so opredeljene tako, da se lahko certifikacija vgradi v sistematične varnostne procese, ki jim proizvajalec sledi v fazi razvoja in v življenjskem ciklu zadevnega izdelka, postopka ali storitve, ali na njih temelji***;

Predlog spremembe 188

Predlog uredbe
Člen 47 – odstavek 1 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) informacije o znanih kibernetskih grožnjah, ki niso zajete v certifikaciji, in smernice, kako jih obravnavati;

Predlog spremembe 189

Predlog uredbe
Člen 47 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) eno ali več stopenj zagotovil, kadar je to ustrezno;	(c) eno ali več stopenj zagotovil, kadar je to ustrezno***, pri čemer se upošteva tudi pristop, ki temelji na tveganju;***

Predlog spremembe 190

Predlog uredbe
Člen 47 – odstavek 1 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) navedbo o tem, ali je lastna izjava o skladnosti dovoljena v shemi, in veljavni postopek za ugotavljanje skladnosti ali lastno izjavo o skladnosti ali oboje;

Predlog spremembe 191

Predlog uredbe
Člen 47 – odstavek 1 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) posebna merila ***in metode*** za ocenjevanje, ***vključno z vrstami ocene***, ki se uporabljajo za dokazovanje, da so posebni cilji iz člena 45 doseženi;	(d) posebna merila za ocenjevanje, ***vrste ugotavljanja skladnosti in metode***, ki se uporabljajo za dokazovanje, da so posebni cilji iz člena 45 doseženi;

Predlog spremembe 192

Predlog uredbe
Člen 47 – odstavek 1 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) informacije, ki jih vložnik predloži organom za ugotavljanje skladnosti in so potrebne za certificiranje;	(e) informacije, ki jih vložnik predloži organom za ugotavljanje skladnosti in so potrebne za certificiranje;

Predlog spremembe 193

Predlog uredbe
Člen 47 – odstavek 1 – točka f

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(f) ***če shema zajema oznake ali znake, pogoje, pod katerimi se*** te ***oznake ali znaki lahko uporabijo***;	(f) ***informacije v zvezi s kibernetsko varnostjo v skladu s členom 47a*** te ***uredbe***;

Predlog spremembe 194

Predlog uredbe
Člen 47 – odstavek 1 – točka g

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(g) ***če shema zajema nadzor, pravila*** za spremljanje skladnosti z zahtevami certifikatov, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;	(g) ***pravila*** za spremljanje skladnosti z zahtevami certifikatov, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;

Predlog spremembe 195

Predlog uredbe
Člen 47 – odstavek 1 – točka h

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(h) pogoje za izdajo, ohranitev, nadaljevanje, razširitev in zmanjšanje področja uporabe ***certificiranja***;	(h) pogoje za izdajo, ohranitev, nadaljevanje, ***pregled,*** razširitev in zmanjšanje področja uporabe ***in rok veljavnosti certifikata***;

Predlog spremembe 196

Predlog uredbe
Člen 47 – odstavek 1 – točka h a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ha) pravila za obravnavanje ranljivosti, ki se lahko pojavijo po izdaji certifikata z vzpostavitvijo dinamičnega in neprekinjenega organizacijskega procesa, ki vključuje ponudnike in uporabnike;

Predlog spremembe 197

Predlog uredbe
Člen 47 – odstavek 1 – točka i

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(i) pravila glede posledic neskladnosti certificiranih izdelkov in storitev IKT s	(i) pravila glede posledic neskladnosti ***samoocenjenih in*** certificiranih izdelkov in

certifikacijskimi zahtevami;	storitev IKT s certifikacijskimi zahtevami;

Predlog spremembe 198

Predlog uredbe
Člen 47 – odstavek 1 – točka j

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(j) pravila glede tega, kako je treba ***predhodno neodkrite*** šibke točke izdelkov in storitev IKT na področju kibernetske varnosti prijaviti in obravnavati;	(j) pravila glede tega, kako je treba šibke točke izdelkov in storitev IKT***, ki niso javno znane,*** na področju kibernetske varnosti prijaviti in obravnavati***, ko se odkrijejo***;

Predlog spremembe 199

Predlog uredbe
Člen 47 – odstavek 1 – točka l

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(l) opredelitev nacionalnih certifikacijskih shem za kibernetsko varnost, ki zadeva isto vrsto ali kategorije izdelkov in storitev IKT;	(l) opredelitev nacionalnih ***ali mednarodnih*** certifikacijskih shem za kibernetsko varnost, ki zadeva isto vrsto ali kategorije izdelkov***, postopkov*** in storitev IKT***, varnostnih zahtev ter meril in metod za ocenjevanje***;

Predlog spremembe 200

Predlog uredbe
Člen 47 – odstavek 1 – točka m a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ma) pogoje za vzajemno priznavanje certifikacijskih shem s tretjimi državami;

Predlog spremembe 201

Predlog uredbe
Člen 47 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Zaradi postopkov vzdrževanja, ki vključujejo posodobitve, se certifikat ne razveljavi, razen če imajo take posodobitve znaten negativni učinek na varnost izdelka, postopka ali storitve IKT.

Predlog spremembe 202

Predlog uredbe
Člen 47 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 47a
	Informacije o kibernetski varnosti za certificirane izdelke, postopke in storitve
	1. Proizvajalec ali dobavitelj izdelkov, postopkov in storitev IKT, ki spada v certifikacijsko shemo v skladu s to uredbo, končnemu uporabniku predloži dokument v elektronski ali papirni obliki, ki vsebuje vsaj naslednje informacije: stopnjo zagotovila certifikata v zvezi s predvideno uporabo izdelka, postopka ali storitve IKT; opis tveganj, pri katerih se s certificiranjem potrdi zaupanje v odpornost proti njim; priporočila o tem, kako lahko uporabniki še naprej spodbujajo kibernetsko varnost izdelka, postopka ali storitve, rednost in obdobje podpore po posodobitvah; po potrebi informacije o tem, kako lahko uporabniki ohranijo glavne značilnosti izdelka, postopka ali storitve v primeru napada.
	2. Dokument iz odstavka 1 tega člena je na voljo v celotnem življenjskem ciklu izdelka, postopka ali storitev do njegovega umika s trga in najmanj pet let.
	3. Komisija sprejme izvedbene akte, s katerimi določi predlogo dokumenta. Komisija lahko od Agencije zahteva, da pripravi predlogo. Navedeni izvedbeni akt se sprejme v skladu s postopkom pregleda

iz člena 55 te uredbe.

Predlog spremembe 203

Predlog uredbe
Člen 48 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Za izdelke in storitve IKT, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete v skladu s členom 44, se domneva, da so skladni z zahtevami take sheme.	1. Za izdelke***, postopke*** in storitve IKT, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete v skladu s členom 44, se domneva, da so skladni z zahtevami take sheme.

Predlog spremembe 204

Predlog uredbe
Člen 48 – odstavek 4 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Z odstopanjem od odstavka 3 in v ustrezno utemeljenih primerih lahko določena evropska shema za kibernetsko varnost določa, da lahko evropski certifikat kibernetske varnosti, ki izhaja iz te sheme, izda le javni organ. Tak javni organ je ***eden od naslednjih:***	4. Z odstopanjem od odstavka 3 in ***samo*** v ustrezno utemeljenih primerih***, kot so razlogi nacionalne varnosti,*** lahko določena evropska ***certifikacijska*** shema za kibernetsko varnost določa, da lahko evropski certifikat kibernetske varnosti, ki izhaja iz te sheme, izda le javni organ. Tak javni organ je ***akreditiran kot organ za ugotavljanje skladnosti v skladu s členom 51(1) te uredbe. Fizična ali pravna oseba, ki predloži svoje izdelke ali storitve IKT certifikacijskemu mehanizmu, organu za ugotavljanje skladnosti iz člena 51 zagotovi vse informacije, ki so potrebne za izvedbo certifikacijskega postopka.***

Predlog spremembe 205

Predlog uredbe
Člen 48 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Fizična ali pravna oseba, ki predloži svoje izdelke ali ***storitve*** IKT certifikacijskemu mehanizmu, organu za ugotavljanje skladnosti iz člena 51 predloži vse informacije, ki so potrebne za izvedbo certifikacijskega postopka.	5. Fizična ali pravna oseba, ki predloži svoje izdelke***, storitve*** ali ***postopke*** IKT certifikacijskemu mehanizmu, organu za ugotavljanje skladnosti iz člena 51 predloži vse informacije, ki so potrebne za izvedbo certifikacijskega postopka***, vključno z informacijami o morebitnih znanih varnostnih ranljivostih. Predloži jih lahko kateremu koli organu za ugotavljanje skladnosti iz člena 51.***

Predlog spremembe 206

Predlog uredbe
Člen 48 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Certifikat se izda za obdobje ***največ treh*** let in se lahko pod enakimi pogoji podaljša, če so zadevne zahteve še vedno izpolnjene.	6. Certifikat se izda za obdobje***, ki se za vsako shemo določi od primera do primera, ob upoštevanju razumnega življenjskega cikla, ki v nobenem primeru ne sme preseči petih*** let in se lahko pod enakimi pogoji podaljša, če so zadevne zahteve še vedno izpolnjene.

Obrazložitev

To zagotavlja prožnost za prilagoditev obdobja veljavnosti predvideni uporabi.

Predlog spremembe 207

Predlog uredbe
Člen 48 – odstavek 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
7. ***Evropski*** certifikat kibernetske varnosti, izdan v skladu s tem členom, se ***prizna*** v vseh državah članicah.	7. ***Za evropski*** certifikat kibernetske varnosti, izdan v skladu s tem členom, se v vseh državah članicah ***prizna, da izpolnjuje lokalne zahteve glede kibernetske varnosti za izdelke in postopke IKT ter elektronske naprave za široko porabo, ki jih ta certifikat zajema, pri čemer se upošteva določena stopnja zagotovila iz člena 46, in se ne razlikuje***

med certifikati na podlagi države članice izvora ali organa za ugotavljanje skladnosti iz člena 51, ki ga je izdal.

Obrazložitev

Da bi se izognili razdrobljenosti pri priznavanju in/ali skladnosti evropskih certifikacijskih shem za kibernetsko varnost, je treba v členu poudariti, da izdaja certifikata ne sme biti predmet diskriminacije.

Predlog spremembe 208

Predlog uredbe
Člen 48 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 48a
	Certifikacijske sheme za izvajalce bistvenih storitev
	1. Ko so evropske certifikacijske sheme za kibernetsko varnost sprejete v skladu z odstavkom 2 tega člena, izvajalci bistvenih storitev za izpolnjevanje varnostnih zahtev, ki izhajajo iz člena 14 Direktive (EU) 2016/1148, uporabljajo izdelke, postopke in storitve, ki jih zajemajo navedene certifikacijske sheme.
	2. Komisija do ... [eno leto po začetku veljavnosti te uredbe] po posvetovanju s skupino za sodelovanje iz člena 11 Direktive (EU) 2016/1148 sprejme delegirane akte v skladu s členom 55a, s katerimi dopolni to uredbo z navedbo kategorij izdelkov, postopkov in storitev, ki izpolnjujejo obe naslednji merili:
	(a) so namenjeni uporabi pri izvajalcih bistvenih storitev; in
	(b) bi njihovo nepravilno delovanje imelo pomemben negativen vpliv na zagotavljanje bistvenih storitev.
	3. Komisija sprejme delegirane akte v skladu s členom 55a za spremembo te uredbe, tako da po potrebi posodobi seznam kategorij izdelkov, postopkov in storitev iz odstavka 3 tega člena.

	4. Komisija pozove Agencijo, naj pripravi predloge za evropske sheme na področju kibernetske varnosti v skladu s členom 44 (-1) te uredbe za seznam kategorij izdelkov, postopkov in storitev iz odstavkov 2 in 3 tega člena, takoj ko bo ta seznam sprejet ali posodobljen. Certifikati, izdani na podlagi takih evropskih certifikacijskih shem za kibernetsko varnost, imajo visoko stopnjo zagotovila.

Predlog spremembe 209

Predlog uredbe
Člen 48 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 48b
	Uradno nasprotovanje evropskim certifikacijskim shemam za kibernetsko varnost
	1. Če država članica meni, da evropska certifikacijska shema za kibernetsko varnost ne izpolnjuje v celoti zahtev, ki naj bi jih skladno s svojimi cilji izpolnjevala in ki so določeni v ustrezni harmonizacijski zakonodaji Unije, o tem obvesti Komisijo in predloži podrobno obrazložitev. Komisija po posvetovanju z odborom, ustanovljenim v skladu z ustrezno harmonizacijsko zakonodajo Unije, ali po potrebi po drugih oblikah posvetovanja s sektorskimi strokovnjaki, sprejme odločitev glede:
	(a) objave, neobjave ali omejene objave sklicevanj na zadevno evropsko certifikacijsko shemo v Uradnem listu Evropske unije;
	(b) ohranitve, ohranitve z omejitvijo ali umika sklicevanj na zadevno evropsko certifikacijsko shemo v Uradnem listu Evropske unije;
	2. Komisija na svojem spletišču objavi informacije o evropskih certifikacijskih

shemah, ki so bile predmet odločitve iz odstavka 1 tega člena;

3. Komisija obvesti Agencijo o odločitvi iz odstavka 1 tega člena in po potrebi zahteva revizijo zadevne evropske certifikacijske sheme za kibernetsko varnost.

4. Odločitev iz odstavka 1(a) tega člena se sprejme v skladu s svetovalnim postopkom iz člena 55(2) te uredbe.

5. Odločitev iz odstavka 1(b) tega člena se sprejme v skladu s postopkom pregleda iz člena 55(2a novo) te uredbe.

Predlog spremembe 210

Predlog uredbe
Člen 49 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Brez poseganja v odstavek 3 nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, prenehajo učinkovati z datumom, določenim v izvedbenem aktu, sprejetem v skladu s členom 44(4). Obstoječe nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke in storitve IKT, ki jih evropska certifikacijska shema za kibernetsko varnost ne zajema, še naprej obstajajo.	1. Brez poseganja v odstavek 3 nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke***, postopke*** in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, prenehajo učinkovati z datumom, določenim v izvedbenem aktu, sprejetem v skladu s členom 44(4). Obstoječe nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke***, postopke*** in storitve IKT, ki jih evropska certifikacijska shema za kibernetsko varnost ne zajema, še naprej obstajajo.

Predlog spremembe 211

Predlog uredbe
Člen 49 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Države članice ne uvedejo novih nacionalnih certifikacijskih shem za	2. Države članice ne uvedejo novih nacionalnih certifikacijskih shem za

kibernetsko varnost za izdelke in storitve IKT, ki jih zajema veljavna evropska certifikacijska shema za kibernetsko varnost.	kibernetsko varnost za izdelke***, postopke*** in storitve IKT, ki jih zajema veljavna evropska certifikacijska shema za kibernetsko varnost.

Predlog spremembe 212

Predlog uredbe
Člen 49 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Države članice sporočijo Komisiji vse zahteve za pripravo evropskih certifikacijskih shem za kibernetsko varnost in navedejo razloge za njihovo uveljavitev.

Predlog spremembe 213

Predlog uredbe
Člen 49 – odstavek 3 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3b. Države članice na zahtevo pošljejo osnutke nacionalnih certifikacijskih shem za kibernetsko varnost drugim državam članicam, Agenciji ali Komisiji, vsaj v elektronski obliki.

Predlog spremembe 214

Predlog uredbe
Člen 49 – odstavek 3 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3c. Brez poseganja v Direktivo (EU) 2015/1535 države članice v treh mesecih pošljejo odgovor in ustrezno upoštevajo vse ugotovitve, ki so jih prejele od drugih držav članic, Agencije ali Komisije v zvezi z morebitnim osnutkom iz odstavka 3b tega člena.

Predlog spremembe 215

Predlog uredbe
Člen 49 – odstavek 3 d (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3d. Kadar je iz ugotovitev, prejetih v skladu z odstavkom 3c tega člena, razvidno, da bi osnutek nacionalne certifikacijske sheme za kibernetsko varnost verjetno negativno vplival na pravilno delovanje notranjega trga, se država članica prejemnica pred sprejetjem osnutka programa posvetuje z Agencijo in Komisijo ter v največji možni meri upošteva njune ugotovitve.

Predlog spremembe 216

Predlog uredbe
Člen 50 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Za učinkovito izvajanje te uredbe je primerno, da ti organi sodelujejo v ***Evropski*** certifikacijski skupini ***za kibernetsko varnost***, ustanovljeni v skladu s členom 53, na dejaven, učinkovit, uspešen in varen način.	5. Za učinkovito izvajanje te uredbe je primerno, da ti organi sodelujejo v certifikacijski skupini ***držav članic***, ustanovljeni v skladu s členom 53, na dejaven, učinkovit, uspešen in varen način.

Predlog spremembe 217

Predlog uredbe
Člen 50 – odstavek 6 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) spremljajo in izvršujejo uporabo določb iz tega naslova na nacionalni ravni ter ***nadzorujejo*** skladnost certifikatov, ki so jih izdali organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz tega naslova in ustrezne evropske certifikacijske sheme za kibernetsko varnost;	(a) spremljajo in izvršujejo uporabo določb iz tega naslova na nacionalni ravni ter ***preverjajo*** skladnost, ***v skladu s pravili, ki jih je sprejela Evropska certifikacijska skupina za kibernetsko varnost v skladu s točko (da) člena 53(3):***

	i) certifikatov, ki so jih izdali organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz tega naslova in ustrezne evropske certifikacijske sheme za kibernetsko varnost; ***in***
	ii) lastnih izjav o skladnosti, predloženih v okviru sheme za postopke, izdelke ali storitve IKT;

Predlog spremembe 218

Predlog uredbe
Člen 50 – odstavek 6 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) spremljajo in nadzorujejo dejavnosti organov za ugotavljanje skladnosti za namene te uredbe, tudi glede priglasitve organov za ugotavljanje skladnosti in s tem povezanih nalog iz člena 52 te uredbe;	(b) spremljajo***,*** nadzorujejo in ***vsaj vsaki dve leti ocenijo*** dejavnosti organov za ugotavljanje skladnosti za namene te uredbe, tudi glede priglasitve organov za ugotavljanje skladnosti in s tem povezanih nalog iz člena 52 te uredbe;

Predlog spremembe 219

Predlog uredbe
Člen 50 – odstavek 6 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) opravljajo preglede, s katerimi zagotovijo, da se v Uniji uporabljajo enakovredni standardi, in o rezultatih poroča Agenciji in skupini;

Obrazložitev

To pripomore k zagotavljanju enotne ravni storitev in kakovosti po vsej EU in prispeva k preprečevanju prakse „iskanja najugodnejšega certificiranja“.

Predlog spremembe 220

Predlog uredbe
Člen 50 – odstavek 6 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) obravnavajo pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, v ustreznem obsegu preučijo vsebino pritožbe ter pritožnika v razumnem roku obvestijo o napredku in izidih preiskave;	(c) obravnavajo pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, ***ali glede samoocene skladnost,*** v ustreznem obsegu preučijo vsebino pritožbe ter pritožnika v razumnem roku obvestijo o napredku in izidih preiskave;

Predlog spremembe 221

Predlog uredbe
Člen 50 – odstavek 6 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) Agenciji in evropski certifikacijski skupini za kibernetsko varnost poročajo o rezultatih preverjanj iz točke (a) in ugotovitvah skladnosti iz točke (b);

Predlog spremembe 222

Predlog uredbe
Člen 50 – odstavek 6 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) sodelujejo z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za kibernetsko varnost;	(d) sodelujejo z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, ***kot so nacionalni nadzorni organi za varstvo podatkov,*** med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov***, postopkov*** in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za kibernetsko varnost;

Predlog spremembe 223

Predlog uredbe
Člen 50 – odstavek 6 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) sodelujejo z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za ***kibernetsko*** varnost;	(d) sodelujejo z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, ***kot so nacionalni nadzorni organi za varstvo podatkov,*** med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za ***informacijsko*** varnost;

Obrazložitev

Iz mnenja evropskega nadzornika za varstvo podatkov.

Predlog spremembe 224

Predlog uredbe
Člen 50 – odstavek 7 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) da odvzame akreditacijo organom za ugotavljanje skladnosti, ki ne upoštevajo te uredbe;

Predlog spremembe 225

Predlog uredbe
Člen 50 – odstavek 7 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) v skladu z nacionalnim pravom odvzame certifikate, ki niso skladni s to uredbo ali evropsko certifikacijsko shemo za kibernetsko varnost;	(e) v skladu z nacionalnim pravom odvzame certifikate, ki niso skladni s to uredbo ali evropsko certifikacijsko shemo za kibernetsko varnost***, ter o tem ustrezno obvesti nacionalne akreditacijske organe***;

Predlog spremembe 226

Predlog uredbe
Člen 50 – odstavek 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*

8. Nacionalni organi za nadzor nad certificiranjem sodelujejo med seboj in s Komisijo ter si zlasti izmenjujejo informacije, izkušnje in dobre prakse glede certificiranja kibernetske varnosti in tehničnih vprašanj, ki zadevajo kibernetsko varnost izdelkov in storitev IKT.	8. Nacionalni organi za nadzor nad certificiranjem sodelujejo med seboj in s Komisijo ter si zlasti izmenjujejo informacije, izkušnje in dobre prakse glede certificiranja kibernetske varnosti in tehničnih vprašanj, ki zadevajo kibernetsko varnost izdelkov***, postopkov*** in storitev IKT.

Predlog spremembe 227

Predlog uredbe
Člen 50 – odstavek 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	8a. Za vsak nacionalni organ za nadzor nad certificiranjem ter vsakega člana in osebje vsakega nacionalnega organa za nadzor nad certificiranjem velja v skladu s pravom Unije ali pravom države članice v zvezi z vsemi zaupnimi informacijami, s katerimi so se seznanili med opravljanjem nalog ali izvajanjem pooblastil, dolžnost varovanja poklicnih skrivnosti v času njihovega mandata in po njem.

Predlog spremembe 228

Predlog uredbe
Člen 50 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 50a
	Medsebojni strokovni pregled
	Za nacionalne organe za nadzor nad certificiranjem se bodo izvajali medsebojni strokovni pregledi vseh dejavnosti, ki jih izvajajo v skladu s členom 50, in jih bo organizirala Agencija.
	Medsebojno strokovno vrednotenje se izvaja na podlagi zanesljivih in preglednih meril in postopkov vrednotenja, zlasti v zvezi z zahtevami

glede strukture, človeških virov in postopkov, zaupnosti ter pritožb. Določiti je treba ustrezne pritožbene postopke zoper odločitve, ki so bile sprejete kot posledica takega vrednotenja.

Medsebojni strokovni pregled zajema ocenjevanje postopkov, ki jih uporabljajo nacionalni organi za nadzor nad certificiranjem, zlasti postopkov za preverjanje skladnosti certifikatov, postopkov spremljanja in nadzora dejavnosti organov za ugotavljanje skladnosti, strokovne usposobljenosti osebja, pravilnosti pregledov in metodologije inšpekcij ter točnosti rezultatov. Pri medsebojnem strokovnem pregledu se oceni tudi, ali ima zadevni nacionalni organ za nadzor nad certificiranjem dovolj sredstev za ustrezno izvajanje svojih nalog, kot je določeno v členu 50(4).

Medsebojni strokovni pregled nacionalnega organa za nadzor nad certificiranjem opravita dva nacionalna organa za nadzor nad certificiranjem iz drugih držav članic in Komisija ter se izvede najmanj vsakih pet let. Agencija lahko sodeluje pri medsebojnem strokovnem pregledu in se o svojem sodelovanju odloči na podlagi analize ocene tveganj.

Komisija lahko v skladu s členom 55a sprejema delegirane akte za dopolnitev te uredbe z določitvijo načrta medsebojnih strokovnih pregledov, ki pokriva vsaj petletno obdobje, ter opredeli merila v zvezi s sestavo skupine za medsebojni strokovni pregled, zanj uporabljeno metodologijo, roke, pogostnost in druge naloge, povezane z njimi. Komisija pri sprejemanju delegiranih aktov ustrezno upošteva ugotovitve certifikacijske skupine držav članic.

Izid medsebojnega strokovnega pregleda prouči certifikacijska skupina držav članic. Agencija pripravi povzetek izida ter po potrebi zagotovi smernice in

dokumente o dobrih praksah ter jih objavi.

Predlog spremembe 229

Predlog uredbe
Člen 51 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Za visoko stopnjo zagotovila mora organ za ugotavljanje skladnosti poleg akreditacije prejeti tudi uradno obvestilo nacionalnega organa za nadzor nad certificiranjem, da je usposobljen in ima strokovno znanje za ocenjevanje kibernetske varnosti. Nacionalni organ za nadzor nad certificiranjem izvaja redne revizije strokovnega znanja in usposobljenosti priglašenih organov za ugotavljanje skladnosti.

Obrazložitev

Za visoko stopnjo zagotovila je potrebno preverjanje učinkovitosti. Strokovno znanje in usposobljenost organov za ugotavljanje skladnosti, ki izvajajo preskuse učinkovitosti, je treba redno preverjati, da se zlasti zagotovi kakovost preskusov.

Predlog spremembe 230

Predlog uredbe
Člen 51 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Za zagotavljanje uporabe enakovrednih standardov v Uniji se izvajajo revizije, o njihovih rezultatih pa se poroča Agenciji in skupini.

Predlog spremembe 231

Predlog uredbe
Člen 51 – odstavek 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. Če se proizvajalci odločijo za lastno izjavo o skladnosti v skladu s členom 48(3), organ za ugotavljanje skladnosti sprejme dodatne ukrepe za preverjanje notranjih postopkov, ki jih uporablja proizvajalec, da zagotovi skladnost izdelka in/ali storitve z zahtevami evropske certifikacijske sheme za kibernetsko varnost.

Predlog spremembe 232

Predlog uredbe
Člen 52 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Komisija lahko z ***izvedbenimi*** akti opredeli okoliščine, obrazce in postopke priglasitve iz odstavka 1 tega člena. Ti ***izvedbeni*** akti se sprejmejo v skladu s postopkom pregleda iz člena 55(2).	5. Komisija lahko z ***delegiranimi*** akti opredeli okoliščine, obrazce in postopke priglasitve iz odstavka 1 tega člena. Ti ***delegirani*** akti se sprejmejo v skladu s postopkom pregleda iz člena 55(2).

Predlog spremembe 233

Predlog uredbe
Člen 53 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Evropska certifikacijska skupina ***za kibernetsko varnost***	Certifikacijska skupina ***držav članic***
	(Sprememba velja za celotno besedilo; če bo sprejeta, bodo potrebne ustrezne prilagoditve v celotnem besedilu.)

Predlog spremembe 234

Predlog uredbe
Člen 53 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Ustanovi se ***Evropska certifikacijska*** skupina za ***kibernetsko varnost (v nadaljnjem besedilu: skupina)***.	1. Ustanovi se ***certifikacijska skupina držav članic***.

Predlog spremembe 235

Predlog uredbe
Člen 53 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. ***Skupino*** sestavljajo nacionalni organi za nadzor nad certificiranjem. Organe zastopajo vodje ali drugi visoki predstavniki nacionalnih organov za nadzor nad certificiranjem.	2. ***Certifikacijsko skupino držav članic*** sestavljajo nacionalni organi za nadzor nad certificiranjem ***iz vsake države članice***. Organe zastopajo vodje ali drugi visoki predstavniki nacionalnih organov za nadzor nad certificiranjem. ***Člani certifikacijske skupine zainteresiranih strani so lahko povabljeni na seje skupine in sodelujejo pri njenem delu.***

Predlog spremembe 236

Predlog uredbe
Člen 53 – odstavek 3 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. ***Skupina*** opravlja naslednje naloge:	3. ***Certifikacijska skupina držav članic*** opravlja naslednje naloge:

Predlog spremembe 237

Predlog uredbe
Člen 53 – odstavek 3 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) podpira, svetuje in sodeluje z agencijo ***ENISA*** pri pripravi predloge za shemo v skladu s členom 44 te uredbe;	(b) podpira, svetuje in sodeluje z Agencijo pri pripravi predloge za shemo v skladu s členom 44 te uredbe;

Predlog spremembe 238

Predlog uredbe
Člen 53 – odstavek 3 – točka d a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(da) sprejme priporočila, ki določajo pogostost preverjanja certifikatov in samoocenjevanja skladnosti s strani nacionalnih organov za nadzor nad certificiranjem ter merila, razsežnost in obseg teh preverjanj, pa tudi skupna pravila in standarde za poročanje v skladu s členom 50(6);

Predlog spremembe 239

Predlog uredbe
Člen 53 – odstavek 3 – točka e

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(e) prouči zadevni razvoj na področju certificiranja kibernetske varnosti in izmenjuje primere dobrih praks na področju certifikacijskih shem za kibernetsko varnost;	(e) prouči zadevni razvoj na področju certificiranja kibernetske varnosti in izmenjuje ***informacije in*** primere dobrih praks na področju certifikacijskih shem za kibernetsko varnost;

Predlog spremembe 240

Predlog uredbe
Člen 53 – odstavek 3 – točka f a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fa) pospešuje usklajevanje evropskih shem kibernetske varnosti z mednarodno priznanimi standardi, vključno s pregledom obstoječih evropskih shem za kibernetsko varnost, in po potrebi daje priporočila Agenciji v zvezi s sodelovanjem z ustreznimi mednarodnimi organizacijami za standardizacijo, da bi odpravili pomanjkljivosti ali vrzeli v razpoložljivih mednarodno priznanih standardih;

Predlog spremembe 241

Predlog uredbe
Člen 53 – odstavek 3 – točka f b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fb) vzpostavi postopek medsebojnega strokovnega pregleda. Ta proces upošteva zlasti zahtevano tehnično strokovno znanje nacionalnih organov za nadzor nad certificiranjem pri opravljanju njihovih nalog, kot je določeno v členih 48 in 50, ter po potrebi vključuje pripravo smernic in dokumentov o dobrih praksah za izboljšanje skladnosti nacionalnih organov za nadzor nad certificiranjem s to uredbo;

Predlog spremembe 242

Predlog uredbe
Člen 53 – odstavek 3 – točka f c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fc) nadzoruje spremljanje in vzdrževanje certifikatov;

Predlog spremembe 243

Predlog uredbe
Člen 53 – odstavek 3 – točka f d (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fd) upošteva rezultate posvetovanja z zainteresiranimi stranmi, ki je bilo izvedeno pri pripravi predloge za shemo v skladu s členom 44.

Predlog spremembe 244

Predlog uredbe
Člen 53 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Komisija predseduje skupini in ji zagotovi sekretariat, pri čemer ji v skladu s členom 8(a) pomaga agencija ***ENISA***.	4. Komisija predseduje ***certifikacijski skupini držav članic*** in ji zagotovi sekretariat, pri čemer ji v skladu s členom 8(a) pomaga Agencija.

Predlog spremembe 245

Predlog uredbe
Člen 53 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 53a
	Pravica do učinkovitega pravnega sredstva zoper nadzorni organ ali organ za ugotavljanje skladnosti
	1. Brez poseganja v katero koli drugo upravno ali izvensodno sredstvo ima vsaka fizična ali pravna oseba pravico do učinkovitega pravnega sredstva:
	(a) zoper odločitev organa za ugotavljanje skladnosti ali nacionalnega organa za nadzor nad certificiranjem v zvezi z njimi, vključno, kadar je to primerno, v zvezi z izdajo, neizdajo ali priznanjem evropskega certifikata kibernetske varnosti, ki ga ima taka oseba v lasti; in
	(b) kadar nacionalni organ za nadzor nad certificiranjem ne obravnava pritožbe, za katero je pristojen.
	2. Postopek zoper organ za ugotavljanje skladnosti ali za nacionalni organ za nadzor nad certificiranjem se predloži sodiščem države članice, v kateri ima organ za ugotavljanje skladnosti ali nacionalni organ za nadzor nad certificiranjem sedež.

Predlog spremembe 246

Predlog uredbe

Člen 55 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Predlog spremembe 247

Predlog uredbe
Člen 55 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 55a
	Izvajanje prenosa pooblastila
	1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.
	2. Pooblastilo za sprejemanje delegiranih aktov iz členov 44 in 48a se prenese na Komisijo za nedoločen čas od ... [datum začetka veljavnosti temeljnega zakonodajnega akta].
	3. Prenos pooblastila iz členov 44 in 48a lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila, naveden v tem sklepu. Sklep začne učinkovati dan po njegovi objavi v Uradnem listu Evropske unije ali na poznejši datum, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.
	4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016.
	5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

	6. Delegirani akt, sprejet na podlagi členov 44 in 48a začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Predlog spremembe 248

Predlog uredbe
Člen 56 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Komisija najpozneje ***pet let*** po datumu iz člena 58, nato pa ***vsakih pet let*** oceni učinek, uspešnost in učinkovitost Agencije in njenih delovnih praks ter morebitno potrebo po spremembi mandata Agencije kot tudi finančne posledice take spremembe. Pri oceni se upoštevajo vse povratne informacije, ki jih Agencija prejme kot odziv na svoje dejavnosti. Če Komisija meni, da nadaljnji obstoj Agencije glede na zastavljene cilje, mandat in naloge ni več upravičen, lahko predlaga spremembo določb te uredbe, ki se nanašajo na Agencijo.	1. Komisija najpozneje ***dve leti*** po datumu iz člena 58, nato pa ***vsaki dve leti*** oceni učinek, uspešnost in učinkovitost Agencije in njenih delovnih praks ter morebitno potrebo po spremembi mandata Agencije kot tudi finančne posledice take spremembe. Pri oceni se upoštevajo vse povratne informacije, ki jih Agencija prejme kot odziv na svoje dejavnosti. Če Komisija meni, da nadaljnji obstoj Agencije glede na zastavljene cilje, mandat in naloge ni več upravičen, lahko predlaga spremembo določb te uredbe, ki se nanašajo na Agencijo.

Predlog spremembe 249

Predlog uredbe
Člen 56 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Oceni se tudi vpliv, učinkovitost in uspešnost določb naslova III glede ciljev zagotavljanja ustrezne ravni kibernetske varnosti izdelkov in storitev IKT v Uniji ter izboljšanja delovanja notranjega trga.	2. Oceni se tudi vpliv, učinkovitost in uspešnost določb naslova III glede ciljev zagotavljanja ustrezne ravni kibernetske varnosti izdelkov***, postopkov*** in storitev IKT v Uniji ter izboljšanja delovanja notranjega trga.

Predlog spremembe 250

Predlog uredbe
Člen 56 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Med ocenjevanjem se presodi, ali so za dostop do notranjega trga potrebne bistvene zahteve glede kibernetske varnosti, da se prepreči vstop izdelkov, storitev in postopkov na trg Unije, ki ne izpolnjujejo osnovnih zahtev glede kibernetske varnosti.

Predlog spremembe 251

Predlog uredbe
Priloga -I (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	PRILOGA -I
	Ob uvedbi certifikacijskega okvira EU za kibernetsko varnost se bo pozornost verjetno usmerila na področja, ki so neposredno zanimiva, da bi se odzvali na izzive nastajajočih tehnologij. Področje interneta stvari je še posebej zanimivo, saj pokriva zahteve potrošnikov in zahteve industrije. Za vključitev v certifikacijski okvir se predlaga naslednji prednostni seznam:
	(1) Certificiranje storitev v oblaku.
	(2) Certificiranje naprav interneta stvari, kar vključuje:
	a. naprave na posamični ravni, kot so pametne nosljive naprave;
	b. naprave na ravni skupnosti, kot so pametni avtomobili, pametni domovi in medicinski pripomočki;
	c. naprave na ravni družbe, kot so pametna mesta in pametna omrežja.

(3) Industrija 4.0, ki vključuje inteligentne, medsebojno povezane kibernetsko-fizične sisteme, ki avtomatizirajo vse faze industrijske dejavnosti od oblikovanja in proizvodnje do obratovanja, dobavne verige in vzdrževanja.

(4) Certificiranje tehnologij in izdelkov, ki se uporabljajo v vsakdanjem življenju. Takšen primer bi lahko bile naprave za mreženje, kot so hišni internetni usmerjevalniki.

Predlog spremembe 252

Predlog uredbe
Priloga I – odstavek 1 – točka 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Če je organ za ugotavljanje skladnosti v lasti ali v upravljanju javne osebe ali ustanove, sta zagotovljeni in dokumentirani neodvisnost in odsotnost morebitnega nasprotja interesov med organom za nadzor nad certificiranjem in organom za ugotavljanje skladnosti.

Predlog spremembe 253

Predlog uredbe
Priloga I – odstavek 1 – točka 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
8. Organ za ugotavljanje skladnosti je zmožen izvajati vse naloge ugotavljanja skladnosti, ki so mu dodeljene s to uredbo, ne glede na to, ali te naloge izvaja organ za ugotavljanje skladnosti sam ali se izvajajo v njegovem imenu in pod njegovo odgovornostjo.	8. Organ za ugotavljanje skladnosti je zmožen izvajati vse naloge ugotavljanja skladnosti, ki so mu dodeljene s to uredbo, ne glede na to, ali te naloge izvaja organ za ugotavljanje skladnosti sam ali se izvajajo v njegovem imenu in pod njegovo odgovornostjo. ***Vsako podizvajanje ali posvetovanje z zunanjim osebjem se ustrezno dokumentira, ne vključuje posrednikov in je predmet pisnega sporazuma, ki med drugim zajema zaupnost in nasprotja interesov. Zadevni***

	organ za ugotavljanje skladnosti prevzame polno odgovornost za opravljene naloge.

Predlog spremembe 254

Predlog uredbe
Priloga I – odstavek 1 – točka 12

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
12. Zagotovi se nepristranskost organa za ugotavljanje skladnosti, njegovega najvišjega vodstva in osebja za ugotavljanje skladnosti.	12. Zagotovi se nepristranskost organa za ugotavljanje skladnosti, njegovega najvišjega vodstva in osebja za ugotavljanje skladnosti ***ter podizvajalcev***.

Predlog spremembe 255

Predlog uredbe
Priloga I – odstavek 1 – točka 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
15. ***Osebje*** organa za ugotavljanje skladnosti ***je zavezano*** k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog v skladu s to uredbo ali katero koli izvedbeno določbo nacionalne zakonodaje, razen pred pristojnimi organi držav članic, v katerih se izvajajo njegove dejavnosti.	15. ***Organ za ugotavljanje skladnosti in njegovo osebje, odbori, odvisne družbe, podizvajalci ter povezani organi ali osebje zunanjih organov*** organa za ugotavljanje skladnosti ***spoštujejo zaupnost informacij in so zavezani*** k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog v skladu s to uredbo ali katero koli izvedbeno določbo nacionalne zakonodaje, razen ***kadar njihovo razkritje zahteva zakonodaja Unije ali države članice, ki velja za te osebe, razen*** pred pristojnimi organi držav članic, v katerih se izvajajo njegove dejavnosti. ***Lastninske pravice so zaščitene. Organ za ugotavljanje skladnosti vzpostavi dokumentirane postopke v zvezi z zahtevami iz oddelka 15.***

Predlog spremembe 256

Predlog uredbe
Priloga I – odstavek 1 – točka 15 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	15a. Z izjemo oddelka 15 zahteve iz te priloge nikakor ne izključujejo izmenjave tehničnih informacij in regulativnih navodil med organom za ugotavljanje skladnosti in osebo, ki zaprosi za certificiranje ali o tem razmišlja.

Predlog spremembe 257

Predlog uredbe
Priloga I – del 1 – točka 15 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	15b. Organi za ugotavljanje skladnosti delujejo v skladu z vrsto doslednih, poštenih in razumnih pogojev, ob upoštevanju interesov malih in srednjih podjetij, kot so opredeljena v Priporočilu 2003/361/ES v zvezi s pristojbinami.