Evropski parlament
2014-2019

Odbor za državljanske svoboščine, pravosodje in notranje zadeve

2017/0225(COD)

16.3.2018

MNENJE

Odbora za državljanske svoboščine, pravosodje in notranje zadeve

za Odbor za industrijo, raziskave in energetiko

o predlogu uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Pripravljavec mnenja: Jan Philipp Albrecht

PA_Legam

KRATKA OBRAZLOŽITEV

Pripravljavec mnenja pozdravlja predlog Komisije o uredbi o kibernetski varnosti[1], saj bolje opredeljuje vlogo agencije ENISA v spremenjenem ekosistemu informacijske varnosti, razvija ukrepe na področju standardov, certificiranja in označevanja informacijske varnosti ter krepi varnost sistemov, ki temeljijo na IKT, vključno s povezanimi predmeti.

Kljub temu pa meni, da je mogoče uvesti dodatne izboljšave. Trdno je prepričan, da je informacijska varnost bistvenega pomena za varstvo temeljnih pravic državljanov v skladu z Listino EU o temeljnih pravicah in za boj proti kibernetski kriminaliteti ter zaščito demokracije in načela pravne države.

Temeljne pravice: Nezaščiteni sistemi lahko dopuščajo kršitve varstva podatkov ali zlorabe identitete, kar bi lahko posameznikom povzročilo dejansko škodo in stisko ter ogrozilo njihovo življenje, zasebnost, dostojanstvo ali lastnino. Priče so utegnile biti v primeru razkritja domačega naslova denimo izpostavljene ustrahovanju in poškodbam, ženske pa nasilju v družini. V internetu stvari, ki vsebuje tudi fizična sprožila in ne samo senzorje, lahko napadi na informacijske sisteme ogrozijo telesno celovitost in življenje posameznikov. Predlogi sprememb pripravljavca mnenja so osredotočeni zlasti na zaščito členov 1, 2, 3, 6, 7, 8, 11 in 17 Listine EU o temeljnih pravicah. V nastajanju je tudi ustavna sodna praksa, prilagojena sedanjemu digitalnemu svetu, ki posebno „temeljno pravico do zaupnosti in celovitosti informacijsko-tehničnih sistemov“[2] izpeljuje iz splošnih osebnostnih pravic.

Boj proti kibernetski kriminaliteti: Nekatere oblike kaznivih dejanj, storjenih na spletu, kot so lažno predstavljanje (ang. phishing) ali finančne in bančne goljufije, vključujejo zlorabo zaupanja, česar ukrepi informacijske varnosti ne morejo preprečiti – v zvezi s temi oblikami kaznivih dejanj pripravljavec mnenja pozdravlja predlagane redne kampanje ozaveščanja in redne javne izobraževalne kampanje za končne uporabnike, ki jih organizira ENISA. Druge oblike spletnega kriminala vključujejo napade na informacijske sisteme, kot so računalniški vdori ali porazdeljeni napadi za zavrnitev storitve – v zvezi s temi pripravljavec mnenja meni, da bo izboljšanje informacijske varnosti učinkovito okrepilo boj proti kibernetski kriminaliteti ter zlasti njeno preprečevanje.

Demokracija in pravna država: Napadi vlad in nedržavnih akterjev na informacijske sisteme so očitna in vse večja grožnja za demokracijo zaradi njihovega vmešavanja v svobodne in poštene volitve, denimo z manipulacijo dejstev in mnenj, s čimer vplivajo na to, kako državljani volijo, posegajo v volilni postopek ter spreminjajo rezultate volitev ali spodkopavajo zaupanje v integriteto glasovanja.

Pripravljavec mnenja zato v svojem osnutku mnenja odbora LIBE predlaga spremembe k predlogu Komisije, ki se osredotočajo na naslednje pomisleke odbora LIBE:

- Agencija bi morala imeti večjo vlogo pri spodbujanju vseh akterjev evropske informacijske družbe k uvajanju preventivnih tehnologij za močno zasebnost ter

[1] Evropska komisija, predlog uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti), COM(2017)0477.
[2] Nemško ustavno sodišče, sodba z dne 27. februarja 2008, zadevi 1 BvR 370/07 in 1 BvR 595/07.

ukrepov na področju informacijske varnosti;

- Agencija bi morala predlagati politike, s katerimi bi vzpostavila nedvoumne odgovornosti in obveznosti vseh zainteresiranih strani v ekosistemih IKT, kadar bi utegnila opustitev ukrepanja v skladu s potrebno skrbnostjo informacijske varnosti imeti resne posledice za varnost, povzročiti obsežno uničenje okolja ali sprožiti sistemsko finančno ali gospodarsko krizo;

- Agencija bi morala v posvetovanju s strokovnjaki na področju informacijske varnosti predlagati jasne in obvezne osnovne zahteve na področju informacijske varnosti;

- Agencija bi morala predlagati sistem certificiranja informacijske varnosti, ki bo trgovcem IKT omogočal povečati preglednost za potrošnika o možnosti nadgraditve in trajanju podpore s programsko opremo. Sistem certificiranja mora biti dinamičen, saj je varnost proces, ki ga je treba stalno izpopolnjevati;

- Agencija bi morala za proizvajalce proizvodov IKT olajšati in znižati ceno izvajanja načel vgrajene varnosti, in sicer z objavljanjem smernic in primerov najboljše prakse;

- Agencija bi morala na poziv institucij, organov, uradov in agencij Unije ter držav članic za njihovo kritično infrastrukturo izvajati redne preventivne revizije informacijske varnosti (pravica do revizije);

- Agencija bi morala proizvajalcem nemudoma poročati o šibkih točkah na področju varnosti, ki še niso javno znane. Nerazkritih šibkih točk v podjetjih in proizvodih ne bi smela prikrivati ali izkoriščati za lastne namene. Vladni organi z razvojem, kupovanjem in izkoriščanjem stranskih vrat v informacijskih sistemih z davkoplačevalskim denarjem ogrožajo varnost državljanov. Da bi zaščitili druge zainteresirane strani, ki v primeru šibkih točk ravnajo odgovorno, bi morala Agencija predlagati politike za odgovorno izmenjavo informacij o šibkih točkah ničtega dne in drugih vrstah šibkih točk na področju varnosti, ki še niso javno znane, tako da bi olajšala odpravljanje teh šibkih točk;

- da bi EU omogočili nadoknaditi zaostanek za panogo informacijske varnosti v tretjih državah, bi morala Agencija opredeliti in začeti izvajati dolgoročni projekt EU v zvezi z informacijsko varnostjo, in sicer v primerljivem obsegu, kot je bilo v letalskem sektorju storjeno z Airbusom.

V predlogu Komisije bi se bilo treba izogibati izrazu „kibernetska varnost“, saj je pravno nejasen in bi lahko privedel do negotovosti. Namesto tega pripravljavec mnenja predlaga, da se nadomesti z izrazom „informacijska varnost“, da bi izboljšali pravno varnost.

PREDLOGI SPREMEMB

Odbor za državljanske svoboščine, pravosodje in notranje zadeve poziva Odbor za industrijo, raziskave in energetiko kot pristojni odbor, da upošteva naslednje predloge sprememb:

Predlog spremembe 1

Predlog uredbe
Naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
UREDBA EVROPSKEGA PARLAMENTA IN SVETA	UREDBA EVROPSKEGA PARLAMENTA IN SVETA
o Agenciji ***EU za kibernetsko*** varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije ***na področju kibernetske varnosti*** (uredba o ***kibernetski*** varnosti)	o Agenciji ***Evropske unije za*** varnost ***omrežij in informacij*** ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju ***informacijske varnosti*** informacijske in komunikacijske tehnologije (uredba o ***informacijski*** varnosti)
	(sprememba velja za celotno besedilo.)

Obrazložitev

Predpona „kiber-“ izhaja iz znanstvenofantastične literature iz 60. let prejšnjega stoletja in se v zadnjem času uporablja za opisovanje negativnih vidikov spleta (kibernetski napad, kibernetska kriminaliteta itd.), vendar je tudi zelo nejasna. Pripravljavec mnenja predlaga spremembo izraza „kibernetska varnost“ v „informacijsko varnost“ zavoljo pravne gotovosti.

Predlog spremembe 2

Predlog uredbe
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(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	(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 ***informacijsko*** varnost. Omejeno ***in razdrobljeno*** certificiranje zato pomeni

informacije za organizacijske in posamezne uporabnike o lastnostih izdelkov in storitev IKT glede ***kibernetske*** varnosti, kar spodkopava zaupanje v digitalne rešitve.	nezadostne informacije za organizacijske in posamezne uporabnike o lastnostih izdelkov in storitev IKT glede ***informacijske*** varnosti, kar spodkopava zaupanje v digitalne rešitve. ***Omrežja IKT so ključna za digitalne proizvode in storitve, ki imajo potencial, da olajšajo vse vidike življenja državljanov in spodbujajo gospodarsko rast EU. Vzpostavljeni morajo biti bistveni tehnološki temeljniki, na katerih slonijo pomembna področja, kot so e-zdravje, internet stvari, umetna inteligenca, kvantna tehnologija, inteligentni prometni sistemi in napredna proizvodnja, da bi lahko v celoti dosegli vse cilje enotnega digitalnega trga.***

Predlog spremembe 3

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***,*** povezana gospodarstvo in družba, ki sta bolj ranljiva za kibernetske grožnje in napade, ***pa*** potrebujeta boljšo ***in varnejšo*** obrambo. Čeprav so kibernetski napadi pogosto čezmejni, so odzivi politike organov za ***informacijsko*** 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 ***informacijske*** varnosti in odpornosti v Uniji ter sistematično napovedujejo prihodnji razvoj, izzivi in grožnje, tako na ravni Unije kot na svetovni ravni.

Predlog spremembe 4

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 ***informacijske*** 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 ***dosego usklajenega odziva EU in*** večjo ozaveščenost državljanov in podjetij o vprašanjih ***informacijske*** 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 ***informacijske*** varnosti za vse nacionalne trge in sektorje. ***Poleg certificiranja na ravni celotne Unije je na voljo niz prostovoljnih ukrepov, ki so na trgu splošno sprejeti glede na izdelek, storitev, uporabo ali standard. Treba bi jih bilo spodbujati hkrati s pristopom industrije od spodaj navzgor, vključno z uporabo vgrajene varnosti, spodbujanjem mednarodnih standardov in prispevkov k njim.***

Predlog spremembe 5

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 ***informacijske*** 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 grožnje in tveganja ***za informacijsko varnost***. V prizadevanjih za boljšo zaščito evropskih državljanov na spletu je Unija leta 2016 sprejela prvi zakonodajni akt na področju ***informacijske*** 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 ***varnosti*** omrežij in informacij). Direktiva o varnosti omrežij in informacij ***izpolnjuje strategijo za enotni digitalni trg ter skupaj z drugimi instrumenti, kot so Direktiva .../... [o evropskem zakoniku o elektronskih komunikacijah, Uredba (EU) 2016/679 Evropskega parlamenta in Sveta[1a] in Direktiva 2002/58/EC Evropskega parlamenta in Sveta[1b],*** določa zahteve glede nacionalnih zmogljivosti na področju ***informacijske*** 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 ***informacijske*** varnosti.

[1a] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

[1b] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

Predlog spremembe 6

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 nove politike Unije za ***informacijsko*** varnost je treba pregledati mandat agencije ENISA, da bi opredelili njeno vlogo v spremenjenem ekosistemu ***informacijske*** varnosti in zagotovili, da ***prevzame vodilno vlogo, ki bo dejansko izboljšala odzivanje*** Unije na izzive na področju ***informacijske*** varnosti, ki izhajajo iz teh korenito spremenjenih groženj in za katere, kot je ugotovljeno v oceni Agencije, sedanji mandat ne zadostuje.

Predlog spremembe 7

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 izzive na področju ***informacijske*** 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. ***Treba je posvetiti ustrezno pozornost nadaljnji krepitvi zmogljivosti Agencije.***

Obrazložitev

Nujno je treba odpraviti pomanjkljivosti v zmogljivosti Agencije. Prizadevati si moramo tudi za določitev nadaljnjega razvoja Agencije glede na izjemen pomen kibernetske varnosti danes in, kar je še važneje, na njen še večji pomen jutri. Opozoriti je treba na rusko vmešavanje v volitve, vedno večje zmogljivosti velesil in držav po svetu ter neizbežno digitalizacijo pomembnih sektorjev.

Predlog spremembe 8

Predlog uredbe
Uvodna izjava 11 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11a) Izzivi na področju informacijske varnosti so v digitalni dobi pogosto tesno prepleteni z izzivi na področju varstva podatkov, varstva zasebnega življenja in varstva elektronskih komunikacij. Da bi lahko Agencija ustrezno obravnavala te izzive, bi morala tesno sodelovati in se pogosto posvetovati z organi, ustanovljenimi v skladu z Uredbo (ES) 45/2001 Evropskega parlamenta in Sveta[1a], Uredbo (EU) 2016/679, Direktivo (EU) 2016/680 in Uredbo (ES) 1211/2009,

ter z industrijo in civilno družbo.

[1a] Uredba (ES) 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

Predlog spremembe 9

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. Poleg tega bi moralo delo Agencije temeljiti na prispevkih in sodelovanju zasebnega sektorja ter drugih zadevnih zainteresiranih strani. ***Opredeliti bi bilo treba jasen načrt in*** sklop nalog ***ter ciljev***, ***ki*** naj ***jih*** Agencija doseže***, hkrati pa bi bilo treba ustrezno upoštevati potrebno*** prožnost ***njenega delovanja. Kolikor je mogoče, je treba ohraniti najvišjo stopnjo preglednosti in razširjanja informacij.***

Predlog spremembe 10

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 ***informacijske*** grožnje je jasno, da je treba države članice podpirati s celovitejšim medsektorskim pristopom h krepitvi kibernetske odpornosti.

Predlog spremembe 11

Predlog uredbe
Uvodna izjava 21 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(21a) Komisija bi morala predlagati, da bi uvedli obvezno sodelovanje med državami članicami na področju zaščite kritične informacijske infrastrukture.

Predlog spremembe 12

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	(26) Agencija mora za boljše razumevanje izzivov na področju ***informacijske*** varnosti in z namenom zagotavljanja dolgoročnega strateškega svetovanja državam članicam in institucijam Unije analizirati sedanja in nastajajoča tveganja***, incidente 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

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***.

tematske ocene o pričakovanih družbenih, pravnih, gospodarskih in regulativnih vplivih tehnoloških inovacij na varnost omrežij in informacij, zlasti na ***informacijsko*** varnost. Agencija bi morala poleg tega države članice ter institucije, agencije in organe Unije podpirati pri prepoznavanju novih trendov in preprečevanju težav v zvezi ***z informacijsko*** varnostjo z opravljanjem analiz groženj***, incidentov*** in ***šibkih točk***.

Predlog spremembe 13

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 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	(28) Agencija bi morala prispevati k ozaveščanju javnosti o tveganjih glede ***informacijske*** varnosti in zagotavljati smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom in organizacijam. ***Da bi*** Agencija ***izboljšala splošno raven pripravljenosti in odpornosti,*** bi morala prispevati tudi k spodbujanju najboljših praks in rešitev na ravni posameznikov in organizacij z zbiranjem in analiziranjem dostopnih informacij o pomembnih incidentih ter pripravljanjem poročil, da bi zagotovila smernice za podjetja***,*** državljane ***in zadevne organe na evropski*** in ***nacionalni ravni***. Agencija bi morala poleg tega v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizirati redne kampanje ozaveščanja in redne javne izobraževalne kampanje za končne uporabnike***. Te kampanje bi morale*** spodbujati ***izobraževanje na področju informacijske varnosti in*** varnejše ravnanje posameznikov na spletu ***ter*** povečati ozaveščenost o potencialnih grožnjah v kibernetskem prostoru, vključno s kibernetsko kriminaliteto, kot so ***lažno predstavljanje***, botneti, finančne in bančne

pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav.	goljufije, ***ponaredbe in nezakonita vsebina,*** pa tudi ***zagovarjati varstvo podatkov in*** osnovno ***avtentikacijo, da se prepreči kraja*** podatkov ***in identitete***. Agencija bi morala imeti osrednjo vlogo pri pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav.

Predlog spremembe 14

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 15

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	(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)***, Agencijo za evropski GNSS (GSA)*** in vsemi drugimi agencijami EU, ki se ukvarjajo ***z informacijsko*** varnostjo. Prav tako bi morala sodelovati z ***evropskimi in nacionalnimi*** organi, ki se ukvarjajo z

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.	varstvom podatkov, da bi izmenjevala tehnično znanje in izkušnje ter najboljše prakse kot tudi nudila svetovanje glede vidikov ***informacijske*** 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.

Obrazložitev

Ker se v zvezi s programom Galileo pojavljajo vprašanja kibernetske varnosti, zlasti pri zemeljskih komponentah, sodelovanje z Agencijo za evropski GNSS dejansko krepi vlogo agencije ENISA, hkrati pa povečuje verodostojnost programa Galileo.

Predlog spremembe 16

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 strojne*** in ***programske opreme ter*** ponudnike ***storitev IKT in spletnih*** storitev spodbujati k zvišanju njihovih splošnih varnostnih standardov, da bi vsi uporabniki interneta lahko ustrezno poskrbeli za svojo osebno ***informacijsko*** varnost. Natančneje, ponudniki storitev in proizvajalci izdelkov bi morali umakniti s trga ali reciklirati izdelke in storitve, ki ne izpolnjujejo standardov ***informacijske*** varnosti. Agencija ENISA lahko v sodelovanju s pristojnimi organi razširja informacije o ravni ***informacijske*** varnosti izdelkov in storitev na notranjem trgu ter izdaja opozorila, namenjena ponudnikom storitev in proizvajalcem, s katerimi od njih zahteva, da izboljšajo ***informacijsko***

varnost svojih izdelkov in storitev. ***Agencija bi si morala skupaj z zainteresiranimi stranmi prizadevati za vseevropski pristop k odgovornemu razkrivanju šibkih točk in spodbujati najboljše prakse na tem področju.***

Predlog spremembe 17

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 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. ***Komisija bi morala glede na pomen certifikacijskih zahtev za zagotovitev zaupanja v internet stvari posebej obravnavati izvedbene ukrepe, s katerimi bi zagotovila uskladitev varnostnih standardov za naprave interneta stvari v vsej EU.***

Predlog spremembe 18

Predlog uredbe
Uvodna izjava 50

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(50) Zdaj se certificiranje izdelkov in	(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.

storitev IKT glede ***informacijske*** 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 ***informacijsko*** 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***, in ti postopki lahko za podjetja pomenijo dodatne stroške***. Poleg tega se zdi, da ni usklajenega in celovitega pristopa k horizontalnim vidikom ***informacijske*** 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. ***Pristop za vsak posamezen primer posebej bi moral zagotoviti, da so storitve in izdelki vključeni v ustrezne certifikacijske sheme. Poleg tega je za učinkovito odkrivanje in blažitev tveganj ter preprečevanje povečanja stroškov za proizvajalce potreben pristop na podlagi tveganj.***

Predlog spremembe 19

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	(52) Glede na navedeno je treba vzpostaviti ***usklajen*** evropski certifikacijski okvir za ***informacijsko*** varnost, ki bi določal glavne horizontalne zahteve za evropske certifikacijske sheme za ***informacijsko*** 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

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.

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 ***informacijsko*** 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.

Predlog spremembe 20

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***	(55) Evropske certifikacijske sheme za ***informacijsko*** 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 ***informacijske*** varnosti, ki se nanašajo na vse izdelke in storitve IKT. Izdelki in storitve IKT ter s tem povezane potrebe po ***informacijski*** varnosti so tako raznoliki, ***pa tudi njihov življenjski cikel je tak,*** da je zelo težko oblikovati splošne zahteve glede ***informacijske*** varnosti, ki bi veljale na vseh področjih. Zato je treba sprejeti širok in splošen pojem ***informacijske*** varnosti za namene certificiranja, ki ga dopolnjuje

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.

sklop posebnih ciljev za ***informacijsko*** varnost, ki jih je treba upoštevati pri oblikovanju evropskih certifikacijskih shem za ***informacijsko*** 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 ***ob tesnem posvetovanju z državami članicami in zainteresiranimi stranmi v industriji***, npr. s sklicem na standarde ali tehnične specifikacije. ***Posamezne certifikacijske sheme bi morale biti oblikovane tako, da bi vse sodelujoče v razvoju zadevnih izdelkov in storitev informacijske tehnologije spodbudili k razvoju in sprejetju standardov, norm in načel, ki bi zagotovili najvišjo možno raven varnosti v celotnem življenjskem ciklu.***

Predlog spremembe 21

Predlog uredbe
Uvodna izjava 55 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(55a) Agencija ENISA bi morala razviti certifikacijsko shemo s svetovno razsežnostjo, da bi preprečili prihodnje trgovinske ovire. V postopku oblikovanja meril za certifikacijske sheme bi se morala Agencija vključiti v dialog z zadevnimi partnerji v sektorju, da se zagotovi tržna izvedljivost.

Predlog spremembe 22

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	(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.	ali storitve IKT. Nadalje bi morali Komisijo pooblastiti, da na podlagi predloge za shemo, ki jo predlaga agencija ENISA, sprejme evropsko certifikacijsko shemo za ***informacijsko*** varnost z izvedbenimi akti. Ob upoštevanju splošnega namena in varnostnih ciljev, opredeljenih v tej uredbi, bi moral biti v evropskih certifikacijskih shemah za ***informacijsko*** 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 ***informacijske*** varnosti, vključno z zajetimi kategorijami izdelkov in storitev IKT, podrobno specifikacijo zahtev glede ***informacijske*** varnosti, npr. s sklicem na standarde ali tehnične specifikacije, posebnimi merili in metodami za ocenjevanje ter predvideno stopnjo zagotovila – osnovno, znatno in/ali visoko. ***Stopnje zagotovila bi bilo treba določiti za vsak primer posebej, da bi zagotovili, da so storitve in izdelki IKT vključeni v ustrezne certifikacijske sheme, prav tako pa bi bilo treba upoštevati različne primere posamezne uporabe ter lastno odgovornost in izobraženost uporabnikov.***

Predlog spremembe 23

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	(57) Uporaba evropskega certificiranja informacijske varnosti bi morala ostati prostovoljna, razen če je v zakonodaji Unije ali nacionalni zakonodaji določeno drugače. ***Po tej začetni fazi in glede na napredek pri izvajanju v državah članicah ter kritičnost izdelka ali storitve bodo morda uvedene morebitne obvezne sheme za nekatere izdelke in storitve IKT v postopnem pristopu za prihodnje***

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.

generacije tehnologij in kot odgovor na politične cilje jutrišnjega dne. Da pa bi dosegli cilje te uredbe in preprečili razdrobljenost notranjega trga, bi nacionalne certifikacijske sheme ali postopki za informacijsko varnost za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za informacijsko 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 informacijsko varnost za izdelke in storitve IKT, ki jih že zajema obstoječa evropska certifikacijska shema za informacijsko varnost.

Predlog spremembe 24

Predlog uredbe
Uvodna izjava 58 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(58a) Agencija bi morala oblikovati jasne osnovne zahteve glede informacijske varnosti in jih po potrebi predlagati Komisiji kot morebitne izvedbene akte, in sicer za vse informacijske naprave, ki se prodajajo v Uniji ali izvažajo iz nje. Te zahteve bi bilo treba pregledati vsaki dve leti, da se zagotovijo stalne izboljšave. Z osnovnimi zahtevami glede informacijske varnosti bi morali med drugim zahtevati, da naprave ne vsebujejo znanih šibkih točk na področju varnosti, ki bi jih bilo mogoče izkoristiti, da lahko sprejmejo zaupanja vredne varnostne posodobitve, da prodajalec obvesti pristojne organe o znanih šibkih točkah ter popravi ali nadomesti prizadete naprave, dokler proizvajalec jasno ne sporoči, da bo varnostna podpora za takšne naprave prenehala.

Predlog spremembe 25

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 obveznega certificiranja v drugih aktih Unije.	(b) določa okvir za vzpostavitev evropskih certifikacijskih shem za ***informacijsko*** varnost za zagotavljanje ustrezne ravni ***informacijske*** varnosti izdelkov in storitev IKT v Uniji. Ta okvir se uporablja brez poseganja v posebne določbe glede prostovoljnega ali obveznega certificiranja v drugih aktih Unije.

Obrazložitev

Predlog spremembe jezikovne narave, ki odpravlja pleonazem iz besedila Komisije.

Predlog spremembe 26

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***, zmogljivost*** ali dogodek, ki bi lahko škodljivo vplival na omrežja in informacijske sisteme, njihove uporabnike in prizadete osebe;

Obrazložitev

Dodan je pomemben vidik, predvsem kar zadeva oceno grožnje.

Predlog spremembe 27

Predlog uredbe
Člen 4 – odstavek 3 – pododstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Agencija si prizadeva za opredelitev kritičnih šibkih točk omrežja

	informacijske varnosti Unije kot celote in tudi posameznih držav članic. Če Agencija meni, da je to potrebno, je treba o šibkih točkah obvestiti Evropski parlament.

Predlog spremembe 28

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 čezmejnih incidentov.	5. Agencija krepi zmogljivosti na področju ***informacijske*** varnosti na ravni Unije, da bi dopolnila ***in podprla*** ukrepe držav članic pri preprečevanju kibernetskih groženj in odzivanju nanje, zlasti v primeru čezmejnih incidentov.

Predlog spremembe 29

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, ***tudi*** s prispevanjem k ***oblikovanju evropskih in mednarodnih standardov o informacijski varnosti ter k*** vzpostavitvi in ohranjanju certifikacijskega okvira za ***informacijsko*** varnost na ravni Unije v skladu z naslovom III te uredbe, in tako krepi preglednost zagotovil izdelkov in storitev IKT glede ***informacijske*** varnosti kot tudi zaupanje v digitalni notranji trg.

Predlog spremembe 30

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 visoko raven ozaveščenosti pri vprašanjih v zvezi ***z informacijsko*** varnostjo.

Obrazložitev

Poleg državljanov in podjetij je treba ozaveščati vse zadevne akterje v družbi, tudi oblasti in zakonodajalce. Predlog spremembe namenoma izpušča naslovnika tovrstnih dejavnosti.

Predlog spremembe 31

Predlog uredbe
Člen 5 – odstavek 1 – točka 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 ***informacijske*** 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 obvladovanje tveganj, poročanje o incidentih in izmenjava informacij, ter lažjo izmenjavo najboljših praks med pristojnimi organi v tem oziru;

Predlog spremembe 32

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. pomočjo Evropskemu odboru za varstvo podatkov, ustanovljenim z Uredbo (EU) 2016/679, pri oblikovanju smernic za podrobno opredelitev pogojev na tehnični ravni, ki upravljavcem podatkov omogočajo zakonito uporabo osebnih podatkov za namene informacijske varnosti s ciljem varovanja njihove infrastrukture, in sicer z odkrivanjem in blokiranjem napadov na njihove

informacijske sisteme v okviru:

(i) Uredbe (EU) 2016/679;

(ii) Direktive (EU) 2016/1148 in

(iii) Direktive 2002/58/ES;

Predlog spremembe 33

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. predlaganjem smernic, s katerimi bi zagotovili, da bodo prodajalci proizvodov IKT pri svojih proizvodih in storitvah ravnali s potrebno skrbnostjo za pravočasno odpravo šibkih točk na področju informacijske varnosti, tako da svojih uporabnikov ne bi po nepotrebnem izpostavljali kibernetskim grožnjam;

Predlog spremembe 34

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2c. predlaganjem smernic za vzpostavitev velike odgovornosti in obveznosti za vse zainteresirane strani (vključno s končnimi uporabniki), ki so udeleženi v ekosistemih IKT;

Predlog spremembe 35

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 d (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2d. predlaganjem smernic, v skladu z nacionalno zakonodajo, glede odgovornosti upravljavcev kritičnih

	omrežnih infrastruktur v primeru napada na njihove informacijske sisteme, ki bi prizadel uporabnike zaradi odsotnosti primerne skrbnosti pri nekaterih uporabnikih ali celo pri operaterju, kadar operater ne ravna dovolj razumno, da bi incident preprečil ali ublažil njegove posledice za vse uporabnike;

Predlog spremembe 36

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 e (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2e. predlaganjem smernic, s katerimi se javnim organom omeji nakup in uporaba šibke točke ničtega dne za napade na informacijske sisteme; spodbujanjem revizij programske opreme in financiranjem strokovnjakov;

Predlog spremembe 37

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 f (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2f. predlaganjem smernic, na podlagi katerih bi javni organi, zasebna podjetja, raziskovalci, univerze in druge zainteresirane strani v okviru odgovornega razkritja objavljali vse kritične šibke točke na področju varnosti, ki še niso javno znane;

Predlog spremembe 38

Predlog uredbe
Člen 5 – odstavek 1 – točka 2 g (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2g. predlaganjem smernic za razširitev uporabe preverljive odprtokodne programske opreme za rešitve na področju informacijske tehnologije v javnem sektorju in s tem povezano uporabo avtomatiziranih orodij za lažji pregled izvorne kode ter za enostavnejše preverjanje stranskih vrat in drugih morebitnih šibkih točk na področju varnosti;

Predlog spremembe 39

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

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fa) in po potrebi sodeluje z nacionalnimi nadzornimi organi za varstvo podatkov;

Predlog spremembe 40

Predlog uredbe
Člen 6 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Agencija olajša vzpostavitev in začetek projekta dolgoročne evropske informacijske varnosti, da bi podprli rast neodvisne evropske panoge informacijske varnosti ter vključili informacijsko varnost v ves razvoj na področju informacijske varnosti v EU.

Obrazložitev

ENISA bi morala zakonodajalcem svetovati pri pripravi politik, da bi lahko EU nadoknadila

zaostanek za industrijami informacijske varnosti v tretjih državah. Projekt bi moral biti po obsegu primerljiv s tem, kar je prej že bilo doseženo v letalski industriji (primer Airbus). To je potrebno za razvoj močnejše, suverene in zaupanja vredne evropske panoge IKT (glej študijo Oddelka za znanstvene napovedi (Presoja znanstvenih in tehnoloških izbir (STOA)), PE 614.531).

Predlog spremembe 41

Predlog uredbe
Člen 7 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. 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.	5. Agencija na zahtevo ***države članice*** 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.
Zadevne države članice in Agencija se dogovorijo o obsegu preiskave in postopku, ki ga je treba upoštevati pri njeni izvedbi, pri čemer ne posegajo v kazensko preiskavo istega incidenta, ki še poteka. Preiskava se zaključi s končnim tehničnim poročilom, ki ga pripravi Agencija zlasti na podlagi informacij in pripomb, ki so jih predložile zadevne države članice in podjetja, ter je dogovorjeno z zadevnimi državami članicami. Povzetek poročila s poudarkom na priporočilih za preprečevanje prihodnjih incidentov se sporoči mreži skupin CSIRT.	Zadevne države članice in Agencija se dogovorijo o obsegu preiskave in postopku, ki ga je treba upoštevati pri njeni izvedbi, pri čemer ne posegajo v kazensko preiskavo istega incidenta, ki še poteka***, ali v nacionalne varnostne ukrepe držav članic***. Preiskava se zaključi s končnim tehničnim poročilom, ki ga pripravi Agencija zlasti na podlagi informacij in pripomb, ki so jih predložile zadevne države članice in podjetja, ter je dogovorjeno z zadevnimi državami članicami. Povzetek poročila s poudarkom na priporočilih za preprečevanje prihodnjih incidentov se sporoči mreži skupin CSIRT.

Predlog spremembe 42

Predlog uredbe
Člen 7 – odstavek 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	8a. Agencija na zahtevo institucije, organa, urada ali agencije Unije ali države članice izvaja redne neodvisne revizije informacijske varnosti kritične infrastrukture s ciljem opredelitve morebitnih priporočil za okrepitev njihove odpornosti.

Obrazložitev

ENISA bi morala imeti pooblastila za izvajanje preventivnih revizij informacijske varnosti za vso kritično infrastrukturo organov držav članic ali institucij, agencij itd. EU.

Predlog spremembe 43

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 ***informacijsko*** varnost za izdelke in storitve IKT ***v sodelovanju z industrijo in*** v skladu s členom 44 te uredbe;

Obrazložitev

Na tem področju je sodelovanje z industrijo pomembno.

Predlog spremembe 44

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

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) vzpostavlja sisteme certificiranja, s katerimi prodajalce IKT in ponudnike storitev odvrača od vključevanja skritih stranskih vrat, ki namerno slabijo

	informacijsko varnost komercialnih proizvodov in storitev ter škodljivo vplivajo na celotno varnost interneta.

Obrazložitev

To bi bilo treba priznati kot enega glavnih ciljev sistemov certificiranja.

Predlog spremembe 45

Predlog uredbe
Člen 9 – odstavek 1 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) združuje, organizira in prek namenskega portala da javnosti na voljo informacije o ***kibernetski*** varnosti, ki jih predložijo institucije, agencije in organi Unije;	(d) združuje, organizira in prek namenskega portala da javnosti na voljo informacije o ***informacijski*** varnosti, ki jih predložijo institucije, agencije in organi Unije ***ter jih dajo na voljo države članice ter javne in zasebne zainteresirane strani***;

Predlog spremembe 46

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 ozavešča o tveganjih glede ***informacijske*** varnosti***, širi ustrezne ukrepe za preprečevanje incidentov*** in zagotavlja smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom in organizacijam;

Predlog spremembe 47

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

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ea) vzpostavi mrežo nacionalnih kontaktnih točk za izobraževanje, da se podpre boljše usklajevanje in izmenjava

	najboljših praks med državami članicami na področju izobraževanja in osveščanja v zvezi z informacijsko varnostjo;

Predlog spremembe 48

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 ***in drugimi ustreznimi zainteresiranimi strani*** organizira redne kampanje ozaveščanja za izboljšanje ***informacijske*** varnosti in njene prepoznavnosti v Uniji***;***

Predlog spremembe 49

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

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ga) spodbuja široko uveljavitev močnih ukrepov informacijske varnosti in zanesljivih tehnologij za krepitev zasebnosti pri vseh akterjih na enotnem digitalnem trgu EU kot prvo obrambno linijo pred napadi na informacijske sisteme.

Obrazložitev

Predlog spremembe temelji na mnenju Evropskega nadzornika za varstvo podatkov (za tehnologije za boljše varovanje zasebnosti). Vloge agencije ENISA ne bi smeli omejevati samo na podporo državam članicam, Komisiji in agencijam EU, temveč bi morala postati bolj prepoznavna v panogi in v splošni javnosti.

Predlog spremembe 50

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) svetuje Uniji in državam članicam o potrebah po raziskavah in prednostnih nalogah na ***področjih informacijske*** varnosti ***ter 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 51

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) ***po merilih strokovnosti izbere in imenuje*** izvršnega direktorja in po potrebi podaljša njegov mandat ali ga razreši s položaja v skladu s členom 33 te uredbe;

Predlog spremembe 52

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	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, ***evropske organizacije za standardizacijo,*** znanstveniki s področja ***informacijske*** varnosti in predstavniki pristojnih organov, ki so uradno obveščeni v skladu z [direktivo o evropskem zakoniku o elektronskih komunikacijah], ter organi

podatkov.	pregona in nadzorni organi za varstvo podatkov.

Predlog spremembe 53

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 ***preglede*** na kraju samem pri vseh upravičencih do nepovratnih sredstev, izvajalcih in podizvajalcih, ki so prejeli sredstva Unije od Agencije.

Predlog spremembe 54

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 tega člena se agencija ENISA posvetuje z vsemi ustreznimi zainteresiranimi stranmi in tesno sodeluje s skupino ***in stalno skupino zainteresiranih strani***. Skupina ***in stalna skupina zainteresiranih strani*** agenciji ENISA ***zagotavljata*** pomoč in strokovno svetovanje, ki ju agencija ENISA potrebuje pri pripravi predloge za shemo, vključno s pripravo mnenj, kadar je to potrebno. ***Agencija ENISA lahko po potrebi ustanovi tudi delovno skupino zainteresiranih strani za certifikacijo, ki jo sestavljajo člani stalne skupine zainteresiranih strani in druge ustrezne zainteresirane strani, da se zagotovi strokovno svetovanje na področjih, ki jih zajemajo posamezne predloge za sheme.***

Obrazložitev

Industrijo bi bilo treba s pomočjo postopka posvetovanja vključiti v oblikovanje in pripravo

predlog za sheme, da bi zagotovili strokovno znanje in s tem učinkovito zasnovo shem.

Predlog spremembe 55

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 izvedbene akte v skladu s členom 55(1), ki določajo evropske certifikacijske sheme za ***informacijsko*** varnost za izdelke in storitve IKT, ki izpolnjujejo zahteve iz členov 45, 46 in 47 te uredbe. ***Komisija se lahko pred sprejetjem teh izvedbenih aktov posvetuje z Evropskim odborom za varstvo podatkov in upošteva njegovo mnenje.***

Obrazložitev

Predlog spremembe temelji na mnenju Evropskega nadzornika za varstvo podatkov. Predlog spremembe zagotavlja skladnost med certificiranjem po evropskem certifikacijskem okviru za kibernetsko varnost ter po Splošni uredbi o varstvu podatkov.

Predlog spremembe 56

Predlog uredbe
Člen 46 – odstavek 2 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Osnovna, znatna in visoka stopnja zagotovila ***izpolnjujejo naslednja merila:***	2. Osnovna, znatna in visoka stopnja zagotovila ***se nanašajo na certifikat, izdan v evropski certifikacijski shemi za informacijsko varnost, ki zagotavlja ustrezno stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve IKT v zvezi z informacijsko varnostjo, in so opredeljene s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati tveganje incidentov v zvezi z informacijsko varnostjo.***

Predlog spremembe 57

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;	***črtano***

Predlog spremembe 58

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 sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je bistveno zmanjšati tveganje kibernetskih incidentov;	***črtano***

Predlog spremembe 59

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.	***črtano***

Predlog spremembe 60

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

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) organe za ugotavljanje skladnosti in revizijske organe;

Predlog spremembe 61

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 certifikacijskih shem za ***informacijsko*** varnost ***v skladu s členom 49***, ki zadeva isto vrsto ali kategorije izdelkov in storitev IKT;

Predlog spremembe 62

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,*** in sicer za največ ***pet*** let in se lahko podaljša, če so zadevne zahteve še vedno izpolnjene.

Predlog spremembe 63

Predlog uredbe
Člen 48 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 48a
	Osnovne zahteve na področju informacijske varnosti
	1. Agencija Komisiji glede na izkušnje s certifikacijskim okvirom za informacijsko varnost v skladu z naslovom III te uredbe predlaga jasne minimalne zahteve na področju informacijske varnosti za vse naprave IT, ki se prodajajo v Uniji ali se iz Unije izvažajo, na primer:
	(a) prodajalec zagotovi pisno potrdilo, da naprava ne vsebuje strojne in programske opreme ali strojnih programskih komponent z znanimi šibkimi točkami na področju varnosti, ki jih je mogoče izkoristiti;
	(b) naprava temelji na programski opremi ali strojnih programskih komponentah, ki so zmožne od proizvajalca sprejeti ustrezno overjene in zaupanja vredne posodobitve;
	(c) naprava ne vsebuje nešifriranega gesla ali dostopne kode; proizvajalec dokumentira možnosti oddaljenega dostopa naprave in jo najkasneje med namestitvijo zavaruje pred nepooblaščenim dostopom; proizvajalec ne zagotovi privzetih strojnih standardnih gesel v napravi; prodajalec dokumentira možnosti uporabnika za posodabljanje naprav in jasno določa odgovornosti v primeru, ko uporabnik naprave ne

posodobi;

(d) prodajalec, distributer in uvoznik z internetom povezanih naprav, programske opreme ali strojnih programskih komponent imajo obveznost, da pristojnemu organu priglasijo morebitne znane šibke točke na področju varnosti, ki jih je mogoče izkoristiti;

(e) proizvajalci z internetom povezanih naprav, programske opreme ali strojnih programskih komponent imajo obveznost, da v primeru novoodkrite šibke točke na področju varnosti zagotovijo popravilo ali zamenjavo;

(f) proizvajalci z internetom povezanih naprav, programske opreme ali strojnih programskih komponent imajo obveznost, da zagotovijo informacije o tem, kako naprava prejema posodobitve v zvezi z informacijsko varnostjo, o predvidenem času za prekinitev podpore v zvezi z informacijsko varnostjo in o postopku za obveščanje uporabnika;

2. Agencija lahko predlaga, da minimalne zahteve v zvezi z informacijsko varnostjo iz odstavka 1 veljajo za naprave IT iz enega ali več posameznih sektorjev.

3. Agencija vsaki dve leti pregleda in po potrebi spremeni zahteve v zvezi z informacijsko varnostjo iz odstavka 1 ter morebitne predloge sprememb posreduje Komisiji kot predloge.

4. Komisija lahko z izvedbenimi akti in na podlagi ocene učinka sklene, da so predlagane ali spremenjene zahteve v zvezi z informacijsko varnostjo iz odstavkov 1 in 2 v Uniji splošno veljavne. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 55(2).

5. Komisija poskrbi za ustrezno javno objavo zahtev v zvezi z informacijsko varnostjo, za katere v skladu z odstavkom 3 sklene, da so splošno veljavne.

6. Agencija zbira vse predlagane

zahteve v zvezi z informacijsko varnostjo in njihove predloge sprememb v registru in jih javno objavi na ustrezne načine.

Obrazložitev

Zaradi večje jasnosti nadomešča točko (c) predloga spremembe 19 k osnutku mnenja. Pomembno je ustvariti odporno informacijsko okolje, ki bo varovalo pred kibernetsko kriminaliteto, in zaščititi temeljne pravice uporabnikov informacijske tehnologije. Zato bi bilo treba v tej uredbi določiti visoke cilje glede informacijske varnosti za obvezno osnovno informacijsko varnost v Uniji.

Predlog spremembe 64

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.

POSTOPEK V ODBORU, ZAPROŠENEM ZA MNENJE

Naslov	Uredba o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (ES) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije (Uredba o kibernetski varnosti)
Referenčni dokumenti	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Pristojni odbor Datum razglasitve na zasedanju	ITRE 23.10.2017
Mnenje pripravil Datum razglasitve na zasedanju	LIBE 23.10.2017
Pripravljavec/-ka mnenja Datum imenovanja	Jan Philipp Albrecht 20.11.2017
Obravnava v odboru	25.1.2018 8.3.2018
Datum sprejetja	8.3.2018
Izid končnega glasovanja	+: 35 –: 2 0: 4
Poslanci, navzoči pri končnem glasovanju	Asim Ademov, Jan Philipp Albrecht, Heinz K. Becker, Caterina Chinnici, Rachida Dati, Cornelia Ernst, Kinga Gál, Sylvie Guillaume, Monika Hohlmeier, Filiz Hjusmenova (Filiz Hyusmenova), Dietmar Köster, Barbara Kudrycka, Monica Macovei, Péter Niedermüller, Ivari Padar, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergej Stanišev (Sergei Stanishev), Traian Ungureanu, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Auke Zijlstra
Namestniki, navzoči pri končnem glasovanju	Maria Grapini, Sylvia-Yvonne Kaufmann, Jeroen Lenaers, Andrejs Mamikins, Maite Pagazaurtundúa Ruiz, John Procter, Jaromír Štětina, Josep-Maria Terricabras, Axel Voss, Elisavet Vozemberg-Vrionidi (Elissavet Vozemberg-Vrionidi)
Namestniki (člen 200(2)), navzoči pri končnem glasovanju	Andrea Bocskor, Reimer Böge, André Elissen, Ramón Jáuregui Atondo, Julia Reda, Rainer Wieland, Patricija Šulin

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V ODBORU, ZAPROŠENEM ZA MNENJE

35	+
ALDE	Filiz Hjusmenova (Filiz Hyusmenova), Maite Pagazaurtundúa Ruiz, Cecilia Wikström
ECR	Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Cornelia Ernst
PPE	Asim Ademov, Heinz K. Becker, Andrea Bocskor, Rachida Dati, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Jaromír Štětina, Patricija Šulin, Traian Ungureanu, Elisavet Vozemberg-Vrionidi (Elissavet Vozemberg-Vrionidi), Rainer Wieland
S&D	Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Ramón Jáuregui Atondo, Sylvia-Yvonne Kaufmann, Dietmar Köster, Andrejs Mamikins, Péter Niedermüller, Ivari Padar, Birgit Sippel, Sergej Stanišev (Sergei Stanishev), Josef Weidenholzer
VERTS/ALE	Jan Philipp Albrecht, Julia Reda, Judith Sargentini, Josep-Maria Terricabras

2	-
ENF	André Elissen, Auke Zijlstra

4	0
EFDD	Kristina Winberg
PPE	Reimer Böge, Monika Hohlmeier, Axel Voss

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani