EVROPSKI PARLAMENT 2009 - 2014

Dokument zasedanja

A7-0103/2014

12.2.2014

***I
POROČILO

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Odbor za notranji trg in varstvo potrošnikov

Poročevalec: Andreas Schwab

Pripravljavca mnenja (*):
Pilar del Castillo Vera, Odbor za industrijo, raziskave in energetiko,
Carl Schlyter, Odbor za državljanske svoboščine, pravosodje in notranje zadeve

(*) Pridruženi odbori – člen 50 Poslovnika

Oznake postopkov

*	Postopek posvetovanja
***	Postopek odobritve
***I	Redni zakonodajni postopek (prva obravnava)
***II	Redni zakonodajni postopek (druga obravnava)
***III	Redni zakonodajni postopek (tretja obravnava)

(Vrsta postopka je odvisna od pravne podlage, ki je predlagana v osnutku akta.)

Spremembe osnutka akta

Pri spremembah, ki jih predlaga Parlament, je spremenjeno besedilo k osnutku akta označeno s ***krepkim poševnim tiskom***. Besedilo, zapisano v *navadnem poševnem tisku*, označuje tehničnim službam namenjeni del osnutka akta s predlaganimi popravki, ki se upoštevajo pri pripravi končnega besedila (na primer očitne napake ali izpustitve v zadevni jezikovni različici). O teh popravkih odločajo pristojne tehnične službe.

Glava vsakega predloga spremembe k obstoječemu aktu, ki se ga želi spremeniti z osnutkom akta, vsebuje še tretjo in četrto vrstico. Tretja vrstica navaja obstoječi akt, četrta pa zadevno določbo tega akta. Besedilo, ki povzema določbo obstoječega akta, ki jo Parlament želi spremeniti, medtem ko v osnutku akta ni bila spremenjena, je označeno s **krepkim tiskom**. Morebitni izbrisi tovrstnega besedila so označeni z **[...]**.

VSEBINA

Stran

(*) Pridruženi odbori – člen 50 Poslovnika

OSNUTEK ZAKONODAJNE RESOLUCIJE EVROPSKEGA PARLAMENTA

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Redni zakonodajni postopek: prva obravnava)

Evropski parlament,

– ob upoštevanju predloga Komisije Evropskemu parlamentu in Svetu (COM(2013)0048),

– ob upoštevanju člena 294(2) in člena 114 Pogodbe o delovanju Evropske unije, na podlagi katerih je Komisija Parlamentu podala predlog (C7-0035/2013),

– ob upoštevanju člena 294(3) Pogodbe o delovanju Evropske unije,

– ob upoštevanju člena 55 Poslovnika,

– ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora z dne 22. maja 2013[1],

– ob upoštevanju svoje resolucije z dne 12. septembra 2013 o strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor[2].

– ob upoštevanju poročila Odbora za notranji trg in varstvo potrošnikov ter mnenj Odbora za zunanje zadeve, Odbora za industrijo, raziskave in energetiko ter Odbora za državljanske svoboščine, pravosodje in notranje zadeve (A7-0103/2014),

1. sprejme stališče v prvi obravnavi, kakor je določeno v nadaljevanju;

2. poziva Komisijo, naj zadevo ponovno predloži Parlamentu, če namerava svoj predlog bistveno spremeniti ali nadomestiti z drugim besedilom;

3. naroči svojemu predsedniku, naj stališče Parlamenta posreduje Svetu in Komisiji ter nacionalnim parlamentom.

[1] UL 0, 0.0.0000, str. 0/ še ni objavljeno v Uradnem listu.
[2] Sprejeta besedila, P7_TA(2013)0376.

Predlog spremembe 1

Predlog direktive
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga.	(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni ***za svobodo in splošno varnost državljanov Unije,*** za gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga.

Predlog spremembe 2

Predlog direktive
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Daljnosežnost in ***pogostnost namernih ali naključnih*** varnostnih incidentov se ***povečujeta in pomenita*** veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo gospodarstvu Unije.	(2) Daljnosežnost***, pogostnost*** in ***posledice*** varnostnih incidentov se ***povečujejo in pomenijo*** veliko tveganje za delovanje omrežij in informacijskih sistemov. ***Ti sistemi lahko prav tako postanejo lahka tarča za namerna škodljiva dejanja, namenjena povzročitvi škode ali prekinitvi delovanja sistemov.*** Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in ***vlagateljev,*** povzročijo veliko škodo gospodarstvu Unije ***ter ogrožajo dobrobit državljanov Unije in sposobnost držav članic, da se zaščitijo in zagotovijo varnost kritične infrastrukture***.

Predlog spremembe 3

Predlog direktive
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Ker so najpogostejši vzroki za izpad sistema še vedno nenamerni, na primer naravni vzroki ali človeška napaka, bi morala biti infrastruktura odporna proti namernim in nenamernim prekinitvam, upravljavci kritične infrastrukture pa bi morali izdelati sisteme, ki bi temeljili na odpornosti.

Predlog spremembe 4

Predlog direktive
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Na ravni Unije bi bilo treba vzpostaviti mehanizem za sodelovanje, ki bi ***omogočil*** izmenjavo informacij ter usklajeno odkrivanje in odzivanje na področju varnosti omrežij in informacij (VOI). Za učinkovito in vključujoče delovanje navedenega mehanizma je bistveno, da imajo vse države članice minimalne zmogljivosti in strategijo za zagotavljanje visoke ravni VOI na svojem ozemlju. Minimalne varnostne zahteve bi morale veljati tudi za ***javne uprave in*** upravljavce ***kritičnih informacijskih infrastruktur***, da se spodbuja kultura obvladovanja tveganja in zagotovi poročanje o najresnejših incidentih.	(4) Na ravni Unije bi bilo treba vzpostaviti mehanizem za sodelovanje, ki bi ***omogočal*** izmenjavo informacij ter usklajeno ***preprečevanje,*** odkrivanje in odzivanje na področju varnosti omrežij in informacij (VOI). Za učinkovito in vključujoče delovanje navedenega mehanizma je bistveno, da imajo vse države članice minimalne zmogljivosti in strategijo za zagotavljanje visoke ravni VOI na svojem ozemlju. Minimalne varnostne zahteve bi morale veljati tudi za ***vsaj nekatere tržne*** upravljavce ***informacijske infrastrukture***, da se spodbuja kultura obvladovanja tveganja in zagotovi poročanje o najresnejših incidentih. ***Podjetja, ki kotirajo na borzi, bi bilo treba spodbujati k prostovoljni javni objavi incidentov v njihovih finančnih poročilih. Pravni okvir bi moral temeljiti na potrebi po varovanju zasebnosti in integritete državljanov. Informacijsko omrežje za opozarjanje o kritični infrastrukturi (CIWIN) bi bilo treba razširiti tudi na tržne udeležence, ki jih zajema ta direktiva.***

Predlog spremembe 5

Predlog direktive
Uvodna izjava 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4a) Medtem ko bi morale javne uprave zaradi svojega poslanstva, ki je v interesu javnosti, pokazati primerno skrbnost pri upravljanju in zaščiti lastnih omrežij in informacijskih sistemov, bi se ta direktiva morala osredotočiti na kritično infrastrukturo, bistveno za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energije, prometa, bančništva, infrastrukture finančnega trga ali zdravja. Razvijalci programske opreme in proizvajalci strojne opreme bi morali biti izključeni s področja uporabe te direktive.

Predlog spremembe 6

Predlog direktive
Uvodna izjava 4 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4b) Sodelovanje in usklajevanje med ustreznimi organi Unije in visokim predstavnikom Unije/podpredsednikom Komisije, pristojnim za zunanje zadeve in varnostno politiko ter skupno varnostno in obrambno politiko, in koordinatorjem EU za boj proti terorizmu bi bilo treba zagotoviti v vseh primerih, ko lahko sklepamo, da incident s znatnim vplivom pomeni tveganje zunanje in teroristične narave.

Predlog spremembe 7

Predlog direktive
Uvodna izjava 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(6) Obstoječe zmogljivosti ne zadostujejo za zagotavljanje visoke ravni VOI v Uniji. Raven pripravljenosti v državah članicah je zelo različna, zato so tudi pristopi po Uniji razdrobljeni. Zaradi tega je raven varstva potrošnikov in podjetij neenaka, zmanjšuje pa se tudi skupna raven VOI v Uniji. Pomanjkanje skupnih minimalnih zahtev za ***javne uprave in*** tržne udeležence pa onemogoča vzpostavitev ***svetovnega*** in učinkovitega mehanizma za sodelovanje na ravni Unije.	(6) Obstoječe zmogljivosti ne zadostujejo za zagotavljanje visoke ravni VOI v Uniji. Raven pripravljenosti v državah članicah je zelo različna, zato so tudi pristopi po Uniji razdrobljeni. Zaradi tega je raven varstva potrošnikov in podjetij neenaka, zmanjšuje pa se tudi skupna raven VOI v Uniji. Pomanjkanje skupnih minimalnih zahtev za tržne udeležence pa onemogoča vzpostavitev ***celovitega*** in učinkovitega mehanizma za sodelovanje na ravni Unije. ***Univerze in raziskovalni centri imajo bistveno vlogo pri spodbujanju raziskav, razvoja in inovacij na teh področjih ter bi jim bilo treba zagotoviti ustrezna sredstva.***

Predlog spremembe 8

Predlog direktive
Uvodna izjava 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) Za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov je zato potreben globalni pristop na ravni Unije, ki bi obsegal skupne minimalne zahteve za gradnjo zmogljivosti in njihovo načrtovanje, izmenjavo informacij in usklajevanje ukrepov ter minimalne varnostne zahteve ***za vse zadevne tržne udeležence in javne uprave***.	(7) Za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov je zato potreben globalni pristop na ravni Unije, ki bi obsegal skupne minimalne zahteve za gradnjo zmogljivosti in njihovo načrtovanje, ***razvoj zadostne usposobljenosti na področju kibernetske varnosti,*** izmenjavo informacij in usklajevanje ukrepov ter ***skupne*** minimalne varnostne zahteve***. Skupne minimalne standarde bi bilo treba uporabljati v skladu z ustreznimi priporočili usklajevalnih skupin za kibernetsko varnost (CSGC)***.

Predlog spremembe 9

Predlog direktive
Uvodna izjava 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(8) Določbe te direktive ne bi smele posegati v možnost, da vsaka država članica sprejme potrebne ukrepe za zaščito bistvenih varnostnih interesov, zaščiti javni red in javno varnost ter preiskuje, odkriva in preganja kazniva dejanja. V skladu s členom 346 PDEU države članice niso dolžne zagotoviti informacij, za katere menijo, da bi njihovo razkritje bilo v nasprotju s ključnimi varnostnimi interesi.	(8) Določbe te direktive ne bi smele posegati v možnost, da vsaka država članica sprejme potrebne ukrepe za zaščito bistvenih varnostnih interesov, zaščiti javni red in javno varnost ter preiskuje, odkriva in preganja kazniva dejanja. V skladu s členom 346 PDEU države članice niso dolžne zagotoviti informacij, za katere menijo, da bi njihovo razkritje bilo v nasprotju s ključnimi varnostnimi interesi. ***Države članice niso dolžne razkriti zaupnih informacij EU, kot je določeno v Sklepu Sveta z dne 31. marca 2011 o varnostnih predpisih za varovanje tajnih podatkov EU (2011/292/EU), informacij, za katere veljajo sporazumi o nerazkritju informacij ali neformalni sporazumi o nerazkritju informacij, kot je protokol TLP (Traffic Light Protocol).***

Obrazložitev

Namen predloga spremembe je pojasniti obdelavo zaupnih informacij, ki spadajo v področje uporabe te direktive.

Predlog spremembe 10

Predlog direktive
Uvodna izjava 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba	(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba

izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni, da bo mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije.

izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni ***na podlagi minimalnih zahtev iz te direktive***, da bo mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije ***ter spoštovala in varovala zasebno življenje in osebne podatke***. ***Zato bi morala vsaka država članica upoštevati skupne standarde v zvezi z obliko zapisa in možnostmi izmenjave podatkov, ki so namenjeni izmenjavi in ocenjevanju. Države članice bi morale imeti možnost, da Evropsko agencijo za varnost omrežij in informacij (ENISA) zaprosijo za pomoč pri oblikovanju nacionalnih strategij VOI na podlagi skupnega minimalnega načrta za strategijo VOI.***

Predlog spremembe 11

Predlog direktive
Uvodna izjava 10 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(10a) Glede na razlike v nacionalnih strukturah upravljanja in z namenom varovanja obstoječih sektorskih dogovorov ali nadzornih in regulativnih organov na ravni Unije ter da bi se izognili podvajanju, bi morale imeti države članice možnost imenovati več kot en pristojni nacionalni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov tržnih udeležencev v okviru te direktive. Vendar je za zagotovitev nemotenega čezmejnega sodelovanja in komunikacije nujno, da vsaka država članica brez poseganja v sektorske regulativne ureditve imenuje samo eno nacionalno enotno kontaktno točko, odgovorno za čezmejno sodelovanje na ravni Unije. Če ustavna struktura ali druge ureditve tako zahtevajo, bi morala

država članica imeti možnost imenovati samo en organ za izvajanje nalog pristojnega organa in enotne kontaktne točke. Pristojni organi in enotne kontaktne točke bi morali biti civilni organi, pod popolnim demokratičnim nadzorom in ne bi smeli izpolnjevati nalog na področju obveščevalne dejavnosti, kazenskega pregona ali obrambe ali biti organizacijsko povezani s katero koli obliko organov, dejavnih na omenjenih področjih.

Predlog spremembe 12

Predlog direktive
Uvodna izjava 11

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(11) Vse države članice bi ***morale*** imeti ustrezne tehnične in organizacijske zmogljivosti ***za preprečevanje, odkrivanje, odzivanje in ublažitev incidentov in tveganj*** VOI. Zato bi bilo treba v vseh državah članicah ustanoviti dobro delujoče skupine za odzivanje na računalniške grožnje, ki bi izpolnjevale bistvene zahteve, da se zagotovijo učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter učinkovito sodelovanje na ravni Unije.	(11) Vse države članice ***in tržni udeleženci*** bi ***morali*** imeti ustrezne tehnične in organizacijske zmogljivosti***, da kadar koli preprečijo, odkrijejo in ublažijo incidente in tveganja*** VOI ***ter se nanje odzovejo***. ***Varnostni sistemi javnih uprav morajo biti varni in predmet demokratičnega nadzora in pregleda. Običajno potrebna oprema in zmogljivosti bi morale biti usklajene s skupno dogovorjenimi tehničnimi standardi in standardnimi operativnimi postopki.*** Zato bi bilo treba v vseh državah članicah ustanoviti dobro delujoče skupine za odzivanje na računalniške grožnje ***(CERT)***, ki bi izpolnjevale bistvene zahteve, da se zagotovijo učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter učinkovito sodelovanje na ravni Unije. ***Tem skupinam bi morali omogočiti sodelovanje na podlagi skupnih tehničnih standardov in standardnih operativnih postopkov. Glede na različne značilnosti obstoječih skupin CERT, ki se odzivajo na različne tematske potrebe in akterje, bi morale države članice zagotoviti, da za vse sektorje s seznama tržnih udeležencev, določenega v***

	tej direktivi, storitve zagotavlja najmanj ena skupina CERT. Glede čezmejnega sodelovanja skupin CERT bi morale države članice zagotoviti, da bodo imele na voljo dovolj sredstev za sodelovanje v obstoječih mednarodnih in evropskih mrežah sodelovanja, ki so že vzpostavljene.

Obrazložitev

Zagotoviti je treba interoperabilnost.

Predlog spremembe 13

Predlog direktive
Uvodna izjava 12

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(12) Na podlagi znatnega napredka, doseženega v okviru evropskega foruma držav članic pri spodbujanju razprave in izmenjave dobrih praks, vključno s pripravo načel za sodelovanje v EU pri kibernetskih krizah, bi morale države članice in Komisija oblikovati mrežo, prek katere bi lahko stalno komunicirale in poglobile svoje sodelovanje. Ta varen in učinkovit mehanizem za sodelovanje bi moral omogočiti strukturirano in usklajeno izmenjavo informacij, odkrivanje in odzivanje na ravni Unije.	(12) Na podlagi znatnega napredka, doseženega v okviru evropskega foruma držav članic pri spodbujanju razprave in izmenjave dobrih praks, vključno s pripravo načel za sodelovanje v EU pri kibernetskih krizah, bi morale države članice in Komisija oblikovati mrežo, prek katere bi lahko stalno komunicirale in poglobile svoje sodelovanje. Ta varen in učinkovit mehanizem za sodelovanje***, po potrebi z udeležbo tržnih udeležencev,*** bi moral omogočiti strukturirano in usklajeno izmenjavo informacij, odkrivanje in odzivanje na ravni Unije.

Predlog spremembe 14

Predlog direktive
Uvodna izjava 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(13) ***Evropska agencija za varnost omrežij in informacij (***ENISA***)*** bi morala državam članicam in Komisiji pomagati s strokovnim znanjem in svetovanjem ter	(13) ENISA bi morala državam članicam in Komisiji pomagati s strokovnim znanjem in svetovanjem ter spodbujati izmenjavo najboljših praks Komisija ***in***

spodbujati izmenjavo najboljših praks**.** Komisija bi se ***morala*** z ENISA posvetovati zlasti pri uporabi te direktive. Da se zagotovi učinkovito in pravočasno obveščanje držav članic in Komisije, bi bilo treba zgodnja opozorila o incidentih in tveganjih priglasiti v mreži za sodelovanje. Da se vzpostavijo zmogljivosti in znanje med državami članicami, bi morala mreža za sodelovanje služiti tudi kot orodje za izmenjavo najboljših praks ter z usmerjanjem organizacije medsebojnih pregledov in vaj na področju VOI članom pomagati pri gradnji zmogljivosti.

države članice bi se ***morale*** z ***agencijo*** ENISA posvetovati zlasti pri uporabi te direktive. Da se zagotovi učinkovito in pravočasno obveščanje držav članic in Komisije, bi bilo treba zgodnja opozorila o incidentih in tveganjih priglasiti v mreži za sodelovanje. Da se vzpostavijo zmogljivosti in znanje med državami članicami, bi morala mreža za sodelovanje služiti tudi kot orodje za izmenjavo najboljših praks ter z usmerjanjem organizacije medsebojnih pregledov in vaj na področju VOI članom pomagati pri gradnji zmogljivosti.

Predlog spremembe 15

Predlog direktive
Uvodna izjava 13 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(13a) Kjer je to primerno, bi morale države članice imeti možnost, da pri uporabi določb te direktive izkoristijo ali prilagodijo obstoječe organizacijske strukture ali strategije.

Predlog spremembe 16

Predlog direktive
Uvodna izjava 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) Treba bi bilo vzpostaviti varno infrastrukturo za izmenjavo informacij, ki bi omogočila izmenjavo občutljivih in zaupnih informacij v okviru mreže za sodelovanje. Ne glede na obveznosti držav članic, da incidente in tveganja z evropsko razsežnostjo priglasijo v mreži za sodelovanje, bi moral biti dostop do zaupnih informacij iz drugih držav članic dovoljen samo, če države članice dokažejo, da njihovi tehnični, finančni in človeški	(14) Treba bi bilo vzpostaviti varno infrastrukturo za izmenjavo informacij, ki bi omogočila izmenjavo občutljivih in zaupnih informacij v okviru mreže za sodelovanje. ***V ta namen bi bilo treba v celoti uporabiti obstoječe strukture v Uniji.*** Ne glede na obveznosti držav članic, da incidente in tveganja z evropsko razsežnostjo priglasijo v mreži za sodelovanje, bi moral biti dostop do zaupnih informacij iz drugih držav članic

viri ter postopki in komunikacijska infrastruktura zagotavljajo učinkovito, uspešno in varno sodelovanje v mreži.

dovoljen samo, če države članice dokažejo, da njihovi tehnični, finančni in človeški viri ter postopki in komunikacijska infrastruktura zagotavljajo učinkovito, uspešno in varno sodelovanje v mreži ***ter uporabljajo pregledne metode***.

Predlog spremembe 17

Predlog direktive
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem ter si izmenjevati informacije in najboljše prakse ***v zameno za*** operativno podporo pri incidentih.	(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem ter si ***medsebojno*** izmenjevati informacije in najboljše prakse***, vključno z vzajemno izmenjavo ustreznih informacij,*** operativno podporo ***in strateško analiziranimi informacijami*** pri incidentih. ***Za uspešno spodbujanje izmenjave informacij in najboljših praks je treba zagotoviti, da tržni udeleženci, ki pri tem sodelujejo, zaradi tega ne bodo prikrajšani. Vzpostaviti je treba ustrezne zaščitne ukrepe, ki bodo zagotavljali, da ti udeleženci zaradi sodelovanja ne bodo izpostavljeni večjim tveganjem v zvezi s skladnostjo ali novim obveznostim, ki izhajajo iz zakonodaje na področju – med drugim – konkurence, intelektualne lastnine, varstva podatkov ali kibernetske kriminalitete, ali večjim operativnim ali varnostnim tveganjem.***

Predlog spremembe 18

Predlog direktive
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi ***morali pristojni organi*** vzpostaviti skupno spletišče, na katerem bi ***objavljali*** nezaupne informacije o incidentih in ***tveganjih***.	(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi ***morale enotne kontaktne točke*** vzpostaviti skupno spletišče ***na ravni Unije***, na katerem bi ***objavljale*** nezaupne informacije o incidentih***, tveganjih*** in ***načinih za zmanjšanje tveganj, po potrebi pa tudi svetovale o ustreznih vzdrževalnih ukrepih***. ***Informacije na spletišču bi morale biti dostopne ne glede na napravo, ki se uporablja. Objava osebnih podatkov na tem spletišču bi morala biti omejena le na potrebne podatke in bi morala zagotoviti najvišjo možno raven anonimnosti.***

Predlog spremembe 19

Predlog direktive
Uvodna izjava 18

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(18) Komisija in države članice bi morale zlasti na podlagi nacionalnih izkušenj s področja kriznega upravljanja in v sodelovanju z agencijo ENISA pripraviti načrt za sodelovanje Unije na področju VOI, v katerem bi opredelile mehanizme za sodelovanje pri obvladovanju tveganj in incidentov. Ta načrt bi bilo treba ustrezno upoštevati pri zgodnjem opozarjanju v mreži za sodelovanje.	(18) Komisija in države članice bi morale zlasti na podlagi nacionalnih izkušenj s področja kriznega upravljanja in v sodelovanju z agencijo ENISA pripraviti načrt za sodelovanje Unije na področju VOI, v katerem bi opredelile mehanizme za sodelovanje***, najboljše prakse in vzorce delovanja*** pri ***preprečevanju, odkrivanju in*** obvladovanju tveganj in incidentov ***ter poročanju o njih***. Ta načrt bi bilo treba ustrezno upoštevati pri zgodnjem opozarjanju v mreži za sodelovanje.

Predlog spremembe 20

Predlog direktive
Uvodna izjava 19

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(19) Priglasitev zgodnjega opozarjanja v mreži bi bilo treba zahtevati le, kadar bi obseg in resnost incidenta ali zadevnega tveganja postala ali lahko postala tako pomembna, da bi bilo potrebno obveščanje ali usklajevanje odziva na ravni Unije. Zgodnje opozarjanje bi moralo biti zato omejeno na ***dejanske ali možne*** incidente ali tveganja, ki se hitro povečujejo, presegajo nacionalne zmogljivosti odzivanja ali prizadenejo več kot eno državo članico. Da se omogoči pravilna ocena, bi bilo treba vse informacije, ki so pomembne za oceno tveganja ali incidenta, priglasiti v mreži za sodelovanje.	(19) Priglasitev zgodnjega opozarjanja v mreži bi bilo treba zahtevati le, kadar bi obseg in resnost incidenta ali zadevnega tveganja postala ali lahko postala tako pomembna, da bi bilo potrebno obveščanje ali usklajevanje odziva na ravni Unije. Zgodnje opozarjanje bi moralo biti zato omejeno na incidente ali tveganja, ki se hitro povečujejo, presegajo nacionalne zmogljivosti odzivanja ali prizadenejo več kot eno državo članico. Da se omogoči pravilna ocena, bi bilo treba vse informacije, ki so pomembne za oceno tveganja ali incidenta, priglasiti v mreži za sodelovanje.

Predlog spremembe 21

Predlog direktive
Uvodna izjava 20

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(20) Ko ***pristojni organi*** prejmejo zgodnje opozorilo in njegovo oceno, bi se ***morali*** dogovoriti o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI. ***Pristojne organe*** in Komisijo bi bilo treba obvestiti o ukrepih, sprejetih na nacionalni ravni, ki so posledica usklajenega odziva.	(20) Ko ***enotne kontaktne točke*** prejmejo zgodnje opozorilo in njegovo oceno, bi se ***morale*** dogovoriti o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI. ***Enotne kontaktne točke, agencijo ENISA*** in Komisijo bi bilo treba obvestiti o ukrepih, sprejetih na nacionalni ravni, ki so posledica usklajenega odziva.

Predlog spremembe 22

Predlog direktive
Uvodna izjava 21

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(21) Zaradi globalne narave težav na področju VOI je potrebno tesnejše mednarodno sodelovanje, da se izboljšajo varnostni standardi in izmenjava informacij	(21) Zaradi globalne narave težav na področju VOI je potrebno tesnejše mednarodno sodelovanje, da se izboljšajo varnostni standardi in izmenjava informacij

ter spodbuja skupen globalen pristop za vprašanja VOI.	ter spodbuja skupen globalen pristop za vprašanja VOI. ***Za okvir takšnega mednarodnega sodelovanja bi bilo treba uporabljati določbe Direktive 95/46/ES in Uredbe (ES) št. 45/2001.***

Predlog spremembe 23

Predlog direktive
Uvodna izjava 22

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(22) Odgovornost za zagotavljanje VOI imajo v veliki meri ***javne uprave in*** tržni udeleženci. Kulturo obvladovanja tveganja, ki vključuje oceno tveganja in izvajanje ustreznih varnostnih ukrepov za zadevna tveganja, bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. Vzpostavitev enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.	(22) Odgovornost za zagotavljanje VOI imajo v veliki meri tržni udeleženci. Kulturo obvladovanja tveganja, ***tesnega sodelovanja in zaupanja,*** ki vključuje oceno tveganja in izvajanje ustreznih varnostnih ukrepov za zadevna tveganja ***in incidente***, ***namerne ali naključne,*** bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. Vzpostavitev ***zaupanja vrednih*** enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.

Predlog spremembe 24

Predlog direktive
Uvodna izjava 24

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(24) Te obveznosti bi bilo treba razširiti prek sektorja elektronskih komunikacij, ***da bi veljale tudi za*** glavne ponudnike storitev informacijske družbe, kakor so opredeljeni v Direktivi 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov ter pravil o storitvah informacijske ***družbe***, ki so podlaga za	(24) Te obveznosti bi bilo treba razširiti prek sektorja elektronskih komunikacij ***na upravljavce infrastrukture***, ***ki so močno odvisni od informacijskih in komunikacijskih tehnologij ter so bistveni za vzdrževanje ključnih gospodarskih in družbenih funkcij, kot so električna energija in plin, promet, kreditne institucije, infrastrukture finančnega trga in zdravje. Prekinitve teh omrežij in***

storitve informacijske družbe na podrejenem trgu ali spletne dejavnosti, kot so platforme za e-trgovanje, portali za spletna plačila, družabna omrežja, iskalniki, storitve računalništva v oblaku***,*** prodajalne z aplikacijami. ***Prekinitve teh omogočitvenih storitev informacijske družbe ovirajo zagotavljanje drugih storitev informacijske družbe, ki so odvisne od njih. Razvijalci programske opreme in proizvajalci strojne opreme niso ponudniki storitev informacijske družbe, zato za njih te obveznosti ne veljajo. Navedene obveznosti bi bilo treba razširiti tudi na javne uprave in upravljavce kritične infrastrukture, ki so močno odvisni od informacijskih in komunikacijskih tehnologij ter so bistveni za vzdrževanje ključnih gospodarskih in družbenih funkcij, kot so električna energija in plin, promet, kreditne institucije, borze in zdravje. Prekinitve teh omrežij in informacijskih sistemov bi vplivale na notranji trg.***

informacijskih sistemov bi vplivale na notranji trg. Čeprav obveznosti iz te direktive ne bi smeli razširiti na glavne ponudnike storitev informacijske družbe, kakor so opredeljeni v Direktivi 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov ter pravil o storitvah informacijske ***družbe***[27], ki so podlaga za storitve informacijske družbe na podrejenem trgu ali spletne dejavnosti, kot so platforme za e-trgovanje, portali za spletna plačila, družabna omrežja, iskalniki, storitve računalništva v oblaku ***na splošno ali*** prodajalne z aplikacijami, ***bi ti lahko na prostovoljni osnovi obveščali pristojni organ ali enotno kontaktno točko o varnostnih incidentih na omrežjih, za katere menijo, da je to primerno. Pristojni organ ali enotna kontaktna točka, če je to mogoče, tržnim udeležencem, ki so ju obvestili o incidentu, predstavita strateško analizirane informacije, ki jim bodo pomagale pri premagovanju varnostne grožnje.***

Predlog spremembe 25

Predlog direktive
Uvodna izjava 24 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(24a) Čeprav ponudniki strojne in programske opreme niso tržni udeleženci, primerljivi s tistimi, ki jih zajema ta direktiva, njihovi proizvodi omogočajo varnost omrežnih in informacijskih sistemov. Zato imajo pomembno vlogo, saj tržnim udeležencem omogočajo, da zavarujejo svoje omrežne in informacijske infrastrukture. Ker so proizvodi strojne in programske opreme že podrejeni veljavnim pravilom o odgovornosti za izdelek, bi morale države članice

zagotoviti izvrševanje teh pravil.

Predlog spremembe 26

Predlog direktive
Uvodna izjava 25

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(25) Tehnični in organizacijski ukrepi za ***javne uprave in*** tržne udeležence ne bi smeli predpisovati, da se določen komercialni izdelek IKT oblikuje, razvije ali proizvede na določen način.	(25) Tehnični in organizacijski ukrepi za tržne udeležence ne bi smeli predpisovati, da se določen komercialni izdelek IKT oblikuje, razvije ali proizvede na določen način.

Predlog spremembe 27

Predlog direktive
Uvodna izjava 26

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(26) ***Javne uprave in tržni*** udeleženci bi morali zagotoviti varnost omrežij in sistemov pod ***njihovim*** nadzorom. To bi bila predvsem zasebna omrežja in sistemi, ki jih upravlja njihovo notranje osebje IT ali za katerih varnost skrbi zunanji izvajalec. Obveznosti varovanja in priglasitve bi morale veljati za zadevne tržne udeležence ***in javne uprave*** ne glede na to, ali omrežja in informacijske sisteme vzdržujejo sami ali njihov zunanji izvajalec.	(26) ***Tržni*** udeleženci bi morali zagotoviti varnost omrežij in sistemov pod ***svojim*** nadzorom. To bi bila predvsem zasebna omrežja in sistemi, ki jih upravlja njihovo notranje osebje IT ali za katerih varnost skrbi zunanji izvajalec. Obveznosti varovanja in priglasitve bi morale veljati za zadevne tržne udeležence ne glede na to, ali omrežja in informacijske sisteme vzdržujejo sami ali njihov zunanji izvajalec.

Predlog spremembe 28

Predlog direktive
Uvodna izjava 28

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(28) Pristojni organi bi morali ustrezno pozornost nameniti ohranjanju neuradnih in zanesljivih kanalov za izmenjavo	(28) Pristojni organi ***in enotne kontaktne točke*** bi morali ustrezno pozornost nameniti ohranjanju neuradnih in

informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom, bi bilo treba najti ravnotežje med interesom javnosti, da je obveščena o nevarnostih, ter morebitno škodo za ugled in poslovanje ***javnih uprav in*** tržnih udeležencev, ki priglasijo incidente. Pri izvajanju obveznosti priglasitve bi morali pristojni organi posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne do ustreznega popravila varnosti.

zanesljivih kanalov za izmenjavo informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. ***Pristojni organi in enotne kontaktne točke bi morali proizvajalce in ponudnike storitev prizadetih produktov in storitev IKT obvestiti o incidentih z znatnim vplivom, ki so jim bili priglašeni.*** Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom ***in enotnim kontaktnim točkam***, bi bilo treba najti ravnotežje med interesom javnosti, da je obveščena o nevarnostih, ter morebitno škodo za ugled in poslovanje tržnih udeležencev, ki priglasijo incidente. Pri izvajanju obveznosti priglasitve bi morali pristojni organi ***in enotne kontaktne točke*** posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne do ustreznega popravila varnosti. ***Enotne kontaktne točke praviloma ne bi smele razkrivati osebnih podatkov posameznikov, vpletenih v incidente. Enotne kontaktne točke bi smele osebne podatke razkriti samo v primeru, da je razkritje teh podatkov nujno in sorazmerno glede na zastavljeni cilj.***

Predlog spremembe 29

Predlog direktive
Uvodna izjava 29

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(29) Pristojni organi bi morali imeti potrebna sredstva za opravljanje svojih nalog, vključno s pooblastili za pridobivanje zadostnih informacij od tržnih udeležencev ***in javnih uprav***, da lahko ocenijo raven varnosti omrežij in informacijskih sistemov, ter zanesljivih in izčrpnih podatkov o dejanskih incidentih, ki so vplivali na delovanje omrežij in informacijskih sistemov.	(29) Pristojni organi bi morali imeti potrebna sredstva za opravljanje svojih nalog, vključno s pooblastili za pridobivanje zadostnih informacij od tržnih udeležencev, da lahko ocenijo raven varnosti omrežij in informacijskih sistemov ***in izmerijo število in obseg incidentov***, ter zanesljivih in izčrpnih podatkov o dejanskih incidentih, ki so vplivali na delovanje omrežij in informacijskih sistemov.

Predlog spremembe 30

Predlog direktive
Uvodna izjava 30

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(30) V mnogih primerih so v ozadju incidentov kriminalne dejavnosti. Sum za to je možen tudi, če na začetku še niso dovolj jasnih dokazov. Pri tem bi moralo biti primerno sodelovanje med pristojnimi organi in organi pregona sestavni del učinkovitega in celovitega odzivanja na ogroženost zaradi varnostnih incidentov. Pri spodbujanju varnega in odpornejšega okolja je pomembno zlasti, da se incidenti, za katere obstaja sum, da so resne kriminalne narave, sistematično priglasijo organom kazenskega pregona. Resno kriminalno naravo incidentov bi bilo treba oceniti ob upoštevanju predpisov EU o kibernetski kriminaliteti.	(30) V mnogih primerih so v ozadju incidentov kriminalne dejavnosti. Sum za to je možen tudi, če na začetku še niso dovolj jasnih dokazov. Pri tem bi moralo biti primerno sodelovanje med pristojnimi organi***, enotnimi kontaktnimi točkami*** in organi pregona ***ter sodelovanje z Europolovim centrom za boj proti kibernetski kriminaliteti in agencijo ENISA*** sestavni del učinkovitega in celovitega odzivanja na ogroženost zaradi varnostnih incidentov. Pri spodbujanju varnega in odpornejšega okolja je pomembno zlasti, da se incidenti, za katere obstaja sum, da so resne kriminalne narave, sistematično priglasijo organom kazenskega pregona. Resno kriminalno naravo incidentov bi bilo treba oceniti ob upoštevanju predpisov EU o kibernetski kriminaliteti.

Predlog spremembe 31

Predlog direktive
Uvodna izjava 31

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(31) V številnih primerih je zaradi incidentov kršena varnost osebnih podatkov. ***Zato*** bi morali ***pristojni organi in organi za varstvo*** podatkov ***pri preprečevanju kršitev*** varnosti osebnih podatkov, nastalih zaradi incidentov, ***med seboj*** sodelovati in ***si*** izmenjevati ***pomembne*** informacije. Če varnostni incident pomeni tudi kršitev varstva osebnih podatkov v skladu ***z Uredbo***	(31) V številnih primerih je zaradi incidentov kršena varnost osebnih podatkov. ***Države članice in tržni udeleženci*** bi morali ***shranjene, obdelane ali posredovane osebne podatke zaščititi pred nenamernim ali nezakonitim uničenjem, nenamerno izgubo ali spremembami in nepooblaščenimi ali nezakonitimi oblikami hrambe, dostopa, razkrivanja ali razširjanja ter zagotoviti***

Evropskega parlamenta in Sveta o varstvu ***posameznikov pri obdelavi osebnih*** podatkov ***in o prostem pretoku takih podatkov***, ***države članice varnostne incidente priglasijo z najmanjšo možno*** upravno ***obremenitvijo***. ENISA bi ***lahko sodelovala s pristojnimi organi in organi za varstvo podatkov ter pripravila*** mehanizme ***in predloge*** za izmenjavo informacij***, s katerimi bi odpravila podvajanje obrazca za priglasitev. En sam*** obrazec za priglasitev bi ***omogočil*** lažje poročanje o incidentih, ki se nanašajo na varstvo osebnih podatkov, s čimer bi se zmanjšala upravna obremenitev za podjetja in javne uprave.

izvajanje varnostne politike v zvezi z obdelavo osebnih podatkov***. Da bi preprečili kršitve*** varnosti osebnih podatkov, nastalih zaradi incidentov, ***v skladu z veljavnimi pravili za varstvo podatkov, bi morali pristojni organi, enotne kontaktne točke in organi za varstvo podatkov*** sodelovati in izmenjevati informacije***, kjer je ustrezno tudi s tržnimi udeleženci***. Če varnostni incident pomeni tudi kršitev varstva osebnih podatkov***, ki jo je treba priglasiti*** v skladu ***s pravom Unije*** o varstvu podatkov, ***bi se morala obveznost priglasitve izvesti tako, da bo*** upravno ***breme čim manjše***. ENISA bi ***morala pripraviti*** mehanizme za izmenjavo informacij ***in enoten*** obrazec za priglasitev***, ki*** bi ***omogočal*** lažje poročanje o incidentih, ki se nanašajo na varstvo osebnih podatkov, s čimer bi se zmanjšala upravna obremenitev za podjetja in javne uprave.

Predlog spremembe 32

Predlog direktive
Uvodna izjava 32

Besedilo, ki ga predlaga Komisija

(32) Standardizacija varnostnih zahtev je tržno usmerjen proces. Da se zagotovi usklajena uporaba varnostnih standardov, bi morale države članice spodbujati uporabo in upoštevanje določenih standardov ter tako zagotoviti visoko raven varnosti na ravni Unije. Zato bi ***bilo morda treba pripraviti*** osnutek harmoniziranih standardov v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa

Predlog spremembe

(32) Standardizacija varnostnih zahtev je ***prostovoljen*** tržno usmerjen proces***, ki bi moral tržnim udeležencem omogočiti uporabo alternativnih sredstev za dosego vsaj podobnih rezultatov***. Da se zagotovi usklajena uporaba varnostnih standardov, bi morale države članice spodbujati uporabo in upoštevanje določenih ***interoperabilnih*** standardov ter tako zagotoviti visoko raven varnosti na ravni Unije. Zato ***je treba razmisliti o uporabi odprtih mednarodnih standardov v zvezi z varnostjo omrežij in informacij ali o oblikovanju takih orodij. Dodaten korak naprej*** bi ***lahko bil*** osnutek harmoniziranih standardov v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in

Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in ***Sveta***.	Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in ***Sveta[29]. Zlasti bi bilo treba Evropski inštitut za telekomunikacijske storitve, Evropski odbor za standardizacijo in Evropski odbor za elektrotehnično standardizacijo pooblastiti za predlaganje uspešnih in učinkovitih odprtih varnostnih standardov Unije, pri čemer bi se morali čim bolj izogibati dajanju prednosti določenim tehnologijam, ti standardi pa bi morali biti enostavni za uporabo s strani malih in srednjih tržnih udeležencev. Mednarodne standarde na področju kibernetske varnosti bi bilo treba temeljito preveriti, da bi zagotovili, da niso kompromisna rešitev in da nudijo ustrezno raven varnosti, kar bo tudi zagotovilo, da bo predpisana skladnost s standardi na področju kibernetske varnosti povišala splošno raven kibernetske varnosti v Uniji in ne nasprotno.***
[29] UL L 316, 14.11.12, str. 12.	[29] UL L 316, 14.11.2012, str. 12.

Predlog spremembe 33

Predlog direktive
Uvodna izjava 33

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(33) Komisija bi morala redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim tehnološkim ***in*** tržnim razmeram.	(33) Komisija bi morala ***v posvetovanju z vsemi zainteresiranimi stranmi*** redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim ***družbenim, političnim,***

tehnološkim ***ali*** tržnim razmeram.

Predlog spremembe 34

Predlog direktive
Uvodna izjava 34

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(34) Da bi mreža za sodelovanje dobro delovala, bi bilo treba v skladu s členom 290 PDEU na Komisijo prenesti pooblastilo za ***sprejemanje aktov, v katerih bi ta opredelila merila, ki jih morajo države članice izpolnjevati, da lahko sodelujejo v sistemu za varno izmenjavo*** informacij***, ter določila nadaljnje specifikacije*** dogodkov, ki sprožijo zgodnje opozarjanje***, in opredelila okoliščine, v katerih morajo tržni udeleženci in javne uprave priglasiti incidente***.	(34) Da bi mreža za sodelovanje dobro delovala, bi bilo treba v skladu s členom 290 PDEU na Komisijo prenesti pooblastilo ***v zvezi s skupnim sklopom standardov o medsebojnem povezovanju in varnosti*** za ***infrastrukturo varne izmenjave*** informacij ***in nadaljnjo specifikacijo*** dogodkov, ki sprožijo zgodnje opozarjanje.

Predlog spremembe 35

Predlog direktive
Uvodna izjava 36

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(36) Da se zagotovijo enotni pogoji za izvajanje te direktive, bi bilo treba ***Komisiji podeliti*** izvedbena pooblastila v zvezi s sodelovanjem ***pristojnih organov*** in Komisije v mreži za sodelovanje, ***dostopom do infrastrukture za varno izmenjavo informacij***, načrtom za sodelovanje Unije na področju VOI***,*** oblikami in postopki, ki se uporabljajo za ***obveščanje javnosti o incidentih, ter standardi in/ali tehničnimi specifikacijami, ki se nanašajo na VOI***. Ta pooblastila bi morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel,	(36) Da se zagotovijo enotni pogoji za izvajanje te direktive, bi bilo treba ***na Komisijo prenesti*** izvedbena pooblastila v zvezi s sodelovanjem ***enotnih kontaktnih točk*** in Komisije v mreži za sodelovanje, ***brez poseganja v obstoječe mehanizme sodelovanja na nacionalni ravni***, načrtom za sodelovanje Unije na področju VOI ***ter*** oblikami in postopki, ki se uporabljajo za ***priglasitev incidentov z znatnim vplivom***. Ta pooblastila bi morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo

na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije.	izvajanje izvedbenih pooblastil Komisije.

Obrazložitev

Predlog spremembe nadomešča predlog spremembe 20. Njegov namen je popraviti napako iz predloga Komisije v zvezi z vsebino načrtovanih izvedbenih aktov in odraziti novi predlog spremembe člena 9(3).

Predlog spremembe 36

Predlog direktive
Uvodna izjava 37

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(37) Pri izvajanju te direktive bi se Komisija morala po potrebi povezati z ustreznimi sektorskimi odbori in organi na ravni EU, zlasti na področju električne energije, prometa in ***zdravja***.	(37) Pri izvajanju te direktive bi se Komisija morala po potrebi povezati z ustreznimi sektorskimi odbori in organi na ravni EU, zlasti na področju ***e-uprave,*** energije, prometa***, zdravja*** in ***obrambe***.

Predlog spremembe 37

Predlog direktive
Uvodna izjava 38

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(38) Informacije, ki jih pristojni organ šteje za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, bi bilo treba izmenjati s Komisijo ***in*** drugimi pristojnimi organi le, če je taka izmenjava nujno potrebna za izvajanje te direktive. Izmenjane informacije bi morale biti omejene na obseg, ki ustreza namenu take izmenjave in ***je sorazmeren*** z njo.	(38) Informacije, ki jih pristojni organ ***ali enotna kontaktna točka*** šteje za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, bi bilo treba izmenjati s Komisijo***, njenimi agencijami, ki jih to zadeva, enotnimi kontaktnimi točkami in/ali*** drugimi ***nacionalnimi*** pristojnimi organi le, če je taka izmenjava nujno potrebna za izvajanje te direktive. Izmenjane informacije bi morale biti omejene na obseg, ki ustreza namenu take izmenjave***, je zanjo nujen*** in z njo ***sorazmeren, ter bi morale upoštevati vnaprej določena merila za zaupnost in varnost, v skladu s Sklepom Sveta z dne 31. marca 2011 o varnostnih predpisih za varovanje tajnih podatkov EU***

(2011/292/EU), informacij, za katere veljajo sporazumi o nerazkritju informacij ali neformalni sporazumi o nerazkritju informacij, kot je protokol TLP (Traffic Light Protocol).

Predlog spremembe 38

Predlog direktive
Uvodna izjava 39

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom je morda potrebna obdelava osebnih podatkov. Taka obdelava osebnih podatkov je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in je zato upravičena na podlagi člena 7 Direktive 95/46/ES. V povezavi s temi upravičenimi cilji ne predstavlja nesorazmernega in nedopustnega posega, ki bi ogrožal bistvo pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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.	(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom ***ali enotnim kontaktnim točkam*** je morda potrebna obdelava osebnih podatkov. Taka obdelava osebnih podatkov je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in je zato upravičena na podlagi člena 7 Direktive 95/46/ES. V povezavi s temi upravičenimi cilji ne predstavlja nesorazmernega in nedopustnega posega, ki bi ogrožal bistvo pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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.

Predlog spremembe 39

Predlog direktive
Uvodna izjava 41 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(41a) V skladu s skupno politično izjavo držav članic in Komisije o obrazložitvenih dokumentih z dne 28. septembra 2011 se države članice zavezujejo, da bodo v upravičenih primerih obvestilu o ukrepih za prenos priložile enega ali več dokumentov, v katerih se pojasni razmerje med sestavnimi elementi direktive in ustreznimi deli nacionalnih instrumentov za prenos. Zakonodajalec meni, da je predložitev takšnih dokumentov pri tej direktivi upravičena.

Predlog spremembe 40

Predlog direktive
Člen 1 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno in ***učinkovito*** obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme;	(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno***, učinkovito*** in ***uspešno*** obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme***, ob udeležbi ustreznih zainteresiranih strani***;

Predlog spremembe 41

Predlog direktive
Člen 1 – odstavek 2 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) določa varnostne zahteve za tržne udeležence ***in javne uprave***.	(c) določa varnostne zahteve za tržne udeležence.

Predlog spremembe 42

Predlog direktive
Člen 1 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Ta direktiva prav tako ne posega v Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ter Uredbo Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.	5. Ta direktiva prav tako ne posega v Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ter Uredbo ***(ES) št. 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. ***Vsaka uporaba osebnih podatkov se omeji na obseg, ki je nujno potreben za namene te direktive, podatki pa so karseda (anonimni) oz. popolnoma anonimni.***

Predlog spremembe 43

Predlog direktive
Člen 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 1a
	Varstvo in obdelava osebnih podatkov
	1. Vsaka obdelava osebnih podatkov v državah članicah na podlagi te direktive se izvaja v skladu z Direktivo 95/46/ES in Direktivo 2002/58/ES.
	2. Vsaka obdelava osebnih podatkov s strani Komisije in agencije ENISA na podlagi te uredbe se izvaja v skladu z

Uredbo (ES) št. 45/2001.

3. Vsaka obdelava osebnih podatkov s strani Europolovega Evropskega centra za boj proti kibernetski kriminaliteti za namene te direktive se izvaja v skladu s Sklepom 2009/371/PNZ.

4. Obdelava osebnih podatkov je poštena in zakonita ter strogo omejena na najmanjšo količino podatkov, ki je potrebna za namene, za katere se ti podatki obdelujejo. Osebni podatki se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namen, za katerega se osebni podatki obdelujejo.

5. Priglasitev incidentov iz člena 14 ne posega v določbe in obveznosti v zvezi z obveščanjem o kršitvi varnosti osebnih podatkov iz člena 4 Direktive 2002/58/ES in Uredbe (EU) št. 611/2013.

Predlog spremembe 44

Predlog direktive
Člen 3 – točka 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo ***računalniških*** podatkov ter	(b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo ***digitalnih*** podatkov ter

Predlog spremembe 45

Predlog direktive
Člen 3 – točka 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) ***računalniške*** podatke, ki jih elementi iz točke (a) in (b) shranjujejo, obdelujejo,	(c) ***digitalne*** podatke, ki jih elementi iz točke (a) in (b) shranjujejo, obdelujejo,

pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;	pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

Predlog spremembe 46

Predlog direktive
Člen 3 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da na dani ravni zaupanja prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne preko navedenih omrežij in informacijskih sistemov,	(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da na dani ravni zaupanja prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne preko navedenih omrežij in informacijskih sistemov; ***„varnost“ zajema ustrezne tehnične naprave, rešitve in operativne postopke, ki zagotavljajo izpolnjevanje varnostnih zahtev iz te direktive.***

Predlog spremembe 47

Predlog direktive
Člen 3 – točka 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) „tveganje“ pomeni vsako okoliščino ali dogodek, ki ima lahko negativen učinek na varnost;	(3) „tveganje“ pomeni vsako ***razumno določljivo*** okoliščino ali dogodek, ki ima lahko negativen učinek na varnost;

Predlog spremembe 48

Predlog direktive
Člen 3 – točka 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) „incident“ pomeni ***vsako okoliščino ali***	(4) „incident“ pomeni ***vsak*** dogodek, ki

dogodek, ki ima dejanski negativen učinek na varnost;	ima dejanski negativen učinek na varnost;

Predlog spremembe 49

Predlog direktive
Člen 3 – točka 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(5) „storitev informacijske družbe“ pomeni storitev po točki (2) člena 1 Direktive 98/34/ES;	***črtano***

Predlog spremembe 50

Predlog direktive
Člen 3 – točka 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo analizo***, ublažitev*** in odzivanje ***na incidente***;	(7) „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo ***odkrivanje, preprečevanje,*** analizo in ***zajezitev incidentov ter*** odzivanje ***nanje***;

Predlog spremembe 51

Predlog direktive
Člen 3 – točka 8 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ponudnika storitev informacijske družbe, ki omogočajo zagotavljanje drugih storitev informacijske družbe;Priloga II vsebuje neizčrpen seznam takih ponudnikov;	***črtano***

Predlog spremembe 52

Predlog direktive
Člen 3 – točka 8 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) upravljavca ***kritične*** infrastrukture, ki je bistvena za vzdrževanje ključnih družbenih ***in gospodarskih*** dejavnosti na področjih energetike, prometa, bančništva, ***borze*** in zdravja; Priloga II vsebuje neizčrpen seznam takih upravljavcev;	(b) upravljavca infrastrukture, ki je bistvena za vzdrževanje ključnih ***gospodarskih in*** družbenih dejavnosti na področjih energetike, prometa, bančništva, ***infrastrukture finančnega trga, internetnih izmenjevalnih točk, prehranske verige,*** in zdravja ***ter katere okvara ali uničenje bi znatno vplivala na državo članico zaradi nevzdrževanja teh funkcij***; Priloga II vsebuje neizčrpen seznam takih upravljavcev***, katerih zadevna omrežja ali informacijski sistemi so povezani z njegovimi temeljnimi storitvami***;

Predlog spremembe 53

Predlog direktive
Člen 3 – točka 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(8a) „incident z znatnim vplivom“ pomeni incident, ki vpliva na varnost in neprekinjenost informacijskega omrežja ali sistema ter povzroča velike motnje v ključnih gospodarskih in družbenih funkcijah;

Predlog spremembe 54

Predlog direktive
Člen 3 – točka 11 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11a) „organizirani trg“ pomeni regulirani trg, kakor je opredeljen v točki 14 člena 4 Direktive 2004/39/ES Evropskega parlamenta in Sveta[1a];

[1a] Direktiva 2004/39/ES Evropskega

parlamenta in Sveta z dne 21. aprila 2004 o trgih finančnih instrumentov (UL L 45, 16.2.2005, str. 18).

Obrazložitev

Poenotenje opredelitve z uredbo Evropskega parlamenta in Sveta o trgih finančnih instrumentov in spremembi Uredbe [uredba o infrastrukturi evropskega trga] o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, ki še čaka na sprejetje.

Predlog spremembe 55

Predlog direktive
Člen 3 – točka 11 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11b) „večstranski sistem trgovanja (MTF)“ pomeni večstranski sistem trgovanja, kakor je opredeljen v točki 15 člena 4 Direktive 2004/39/ES;

Obrazložitev

Poenotenje opredelitve z uredbo Evropskega parlamenta in Sveta o trgih finančnih instrumentov in spremembi Uredbe [uredba o infrastrukturi evropskega trga] o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, ki še čaka na sprejetje.

Predlog spremembe 56

Predlog direktive
Člen 3 – točka 11 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11c) „sistem organiziranega trgovanja“ pomeni večstranski sistem ali instrument, ki ni organizirani trg, večstranski sistem trgovanja ali centralna nasprotna stranka, ki ga upravlja investicijsko podjetje ali tržni udeleženec ter v katerem lahko medsebojno vpliva več nakupnih in prodajnih interesov tretjih oseb v zvezi z obveznicami, strukturiranimi finančnimi

	produkti, emisijskimi kuponi ali izvedenimi finančnimi instrumenti tako, da se kot posledica tega sklene pogodba v skladu z določbami naslova II Direktive 2004/39/ES;

Obrazložitev

Vpeljava opredelitve je v skladu z uredbo Evropskega parlamenta in Sveta o trgih finančnih instrumentov in spremembi Uredbe [uredba o infrastrukturi evropskega trga] o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, ki še čaka na sprejetje, in je odvisna od končnega besedila navedene uredbe.

Predlog spremembe 57

Predlog direktive
Člen 5 – odstavek 1 – točka e a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ea) Države članice lahko agencijo ENISA zaprosijo za pomoč pri oblikovanju svojih nacionalnih strategij VOI in nacionalnih načrtov za sodelovanje na področju VOI na podlagi skupne minimalne strategije VOI.

Predlog spremembe 58

Predlog direktive
Člen 5 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ***načrt ocene*** tveganja za ***prepoznavanje*** tveganj ***in ocenjevanje*** učinkov morebitnih incidentov;	(a) ***okvir za obvladovanje*** tveganja za ***vzpostavitev metodologije za opredeljevanje, razvrščanje, oceno in obravnavo*** tveganj***, oceno*** učinkov morebitnih incidentov***, možnosti za preprečevanje in nadzor ter za opredelitev meril za izbiro morebitnih protiukrepov***;

Obrazložitev

Predlog spremembe nadomešča predlog spremembe 29. Predlog Komisije bi bil v zvezi z vprašanji nacionalne varnosti držav članic preveč daljnosežen, načrt za sodelovanje pa bi s

tem postal nepraktičen in preveč kompleksen, da bi bil lahko učinkovit.

Predlog spremembe 59

Predlog direktive
Člen 5 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) opredelitev vloge in odgovornosti različnih akterjev, vključenih v izvajanje ***načrta***;	(b) opredelitev vloge in odgovornosti različnih ***organov in drugih*** akterjev, vključenih v izvajanje ***okvira***;

Predlog spremembe 60

Predlog direktive
Člen 5 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI se sporočita Komisiji v ***enem mesecu*** po sprejetju.	3. Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI se sporočita Komisiji v ***treh mesecih*** po sprejetju.

Predlog spremembe 61

Predlog direktive
Člen 6 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Pristojni nacionalni ***organ*** za varnost omrežij in informacijskih sistemov	Pristojni nacionalni ***organi in enotne kontaktne točke*** za varnost omrežij in informacijskih sistemov

Predlog spremembe 62

Predlog direktive
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica določi ***nacionalni***	1. Vsaka država članica določi ***enega ali***

organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu **„**pristojni organ**“**).	***več civilnih nacionalnih organov, pristojnih*** za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu***:*** pristojni organ).

Obrazložitev

Predlog spremembe nadomesti predlog spremembe 32 in je namenjen dodatni opredelitvi institucije, ki bi morala imeti vlogo pristojnega nacionalnega organa.

Predlog spremembe 63

Predlog direktive
Člen 6 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Če država članica imenuje več kot en pristojni organ, imenuje civilni nacionalni organ, na primer pristojni organ, za enotno nacionalno kontaktno točko za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu: enotna kontaktna točka). Če država članica imenuje samo en pristojni organ, potem je ta pristojni organ tudi enotna kontaktna točka.

Obrazložitev

Predlog spremembe nadomešča predlog spremembe 33 in je skladen z novim predlogom spremembe člena 6(1), ki ga je vložil poročevalec. Namenjen je dodatni opredelitvi institucije, ki bi morala imeti vlogo pristojnega nacionalnega organa.

Predlog spremembe 64

Predlog direktive
Člen 6 – odstavek 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. Pristojni organi in enotna kontaktna točka iste države članice tesno sodelujejo glede obveznosti, ki jih določa ta direktiva.

Predlog spremembe 65

Predlog direktive
Člen 6 – odstavek 2 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2c. Enotna kontaktna točka zagotavlja čezmejno sodelovanje z drugimi enotnimi kontaktnimi točkami.

Predlog spremembe 66

Predlog direktive
Člen 6 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Države članice zagotovijo, da imajo pristojni organi ustrezne tehnične, finančne in človeške vire, da lahko učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnijo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje ***pristojnih organov*** prek mreže iz člena 8.	3. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** ustrezne tehnične, finančne in človeške vire, da lahko učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnijo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje ***enotnih kontaktnih točk*** prek mreže iz člena 8.

Predlog spremembe 67

Predlog direktive
Člen 6 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci pristojnim organom priglasijo dogodke, kot to določa člen 14(2), in da se pristojnim organom podelijo izvedbena in izvršilna pooblastila iz člena 15.	4. Države članice zagotovijo, da tržni udeleženci pristojnim organom ***in enotnim kontaktnim točkam, kjer je to v skladu z odstavkom 2a tega člena,*** priglasijo dogodke, kot to določa člen 14(2), in da se pristojnim organom ***in enotnim kontaktnim točkam*** podelijo izvedbena in izvršilna pooblastila iz člena 15.

Obrazložitev

Predlog spremembe nadomešča predlog spremembe 37. Namenjen je pojasnitvi vlog različnih organov, da bi preprečili podvajanje pri priglasitvah pristojnim organom in enotnim kontaktnim točkam. Ker se v nekaterih sektorjih incidenti že priglasijo organom Unije, bi bilo treba preprečiti podvajanje.

Predlog spremembe 68

Predlog direktive
Člen 6 – odstavek 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4a. Kjer zakonodaja Unije določa specifičen sektorski nadzorni ali regulativni organ na ravni Unije, med drugim za varnost omrežij in informacijskih sistemov, ta organ od zadevnih tržnih udeležencev v sektorju sprejema priglasitve incidentov v skladu s členom 14(2) ter ima pooblastila za izvajanje in izvrševanje iz člena 15. Ta organ Unije v povezavi s temi obveznostmi tesno sodeluje s pristojnimi organi in enotnimi kontaktnimi točkami države članice gostiteljice. Enotne kontaktne točke države članice gostiteljice predstavljajo organ Unije v zvezi z obveznostmi iz poglavja III.

Predlog spremembe 69

Predlog direktive
Člen 6 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi se po potrebi posvetujejo in sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.	5. Pristojni organi ***in enotne kontaktne točke*** se po potrebi posvetujejo in sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.

Predlog spremembe 70

Predlog direktive
Člen 6 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Vsaka država članica Komisijo nemudoma obvesti o imenovanju pristojnih organov, njihovih nalogah in vseh morebitnih poznejših spremembah. Vsaka država članica javno objavi imenovanje ***pristojnega organa***.	6. Vsaka država članica Komisijo nemudoma obvesti o imenovanju pristojnih organov ***in enotne kontaktne točke***, njihovih nalogah in vseh morebitnih poznejših spremembah. Vsaka država članica javno objavi imenovanje ***pristojnih organov***.

Predlog spremembe 71

Predlog direktive
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica ustanovi skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. CERT se lahko ustanovi znotraj pristojnega organa.	1. Vsaka država članica ***za vsakega od sektorjev iz Priloge II*** ustanovi ***vsaj eno*** skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. ***Skupina*** CERT se lahko ustanovi znotraj pristojnega organa.

Predlog spremembe 72

Predlog direktive
Člen 7 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. CERT delujejo pod nadzorom pristojnega organa, ki redno pregleduje ustreznost njihovih virov, pristojnosti in učinkovitosti postopka obravnavanja incidentov.	5. ***Skupine*** CERT delujejo pod nadzorom pristojnega organa ***ali enotne kontaktne točke***, ki redno pregleduje ustreznost njihovih virov, pristojnosti in učinkovitosti postopka obravnavanja incidentov.

Predlog spremembe 73

Predlog direktive
Člen 7 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Države članice zagotovijo, da imajo skupine CERT na voljo zadostne človeške in finančne vire za aktivno sodelovanje v mednarodnih mrežah za sodelovanje in zlasti v mrežah Unije za sodelovanje.

Predlog spremembe 74

Predlog direktive
Člen 7 – odstavek 5 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5b. Skupine CERT lahko dajejo pobude za skupne vaje z drugimi skupinami CERT, s skupinami CERT v vseh državah članicah in z ustreznimi institucijami držav nečlanic ter s skupinami CERT večnacionalnih in mednarodnih institucij, kot sta NATO in OZN; za tovrstne pobude in sodelovanje v skupnih vajah se te skupine tudi spodbuja.

Predlog spremembe 75

Predlog direktive
Člen 7 – odstavek 5 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5c. Pri oblikovanju nacionalnih skupin CERT lahko države članice zaprosijo za pomoč agencijo ENISA ali druge države članice.

Predlog spremembe 76

Predlog direktive
Člen 8 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. ***Pristojni organi*** in Komisija vzpostavijo mrežo („mreža za sodelovanje“), v kateri sodelujejo pri preprečevanju tveganj in incidentov, ki vplivajo na omrežja in informacijske sisteme.	1. ***Enotne kontaktne točke*** in Komisija ***ter agencija ENISA*** vzpostavijo mrežo (***v nadaljnjem besedilu*** „mreža za sodelovanje“), v kateri sodelujejo pri preprečevanju tveganj in incidentov, ki vplivajo na omrežja in informacijske sisteme.

Predlog spremembe 77

Predlog direktive
Člen 8 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in pristojnimi organi. Evropska agencija za varnost omrežij in informacij (ENISA) na zahtevo mreži za sodelovanje pomaga tako, da zagotovi strokovno znanje ter svetovanje.	2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in enotnimi kontaktnimi točkami. Agencija ENISA na zahtevo mreži za sodelovanje pomaga tako, da zagotovi strokovno znanje ter svetovanje. ***Po potrebi so lahko k sodelovanju pri dejavnostih mreže za sodelovanje, navedenih v točkah (g) in (i) odstavka 3, povabljeni tudi tržni udeleženci in ponudniki rešitev glede kibernetske varnosti.*** ***Če je to primerno, mreža za sodelovanje sodeluje z organi za varstvo podatkov.*** ***Komisija mrežo za sodelovanje redno obvešča o raziskavah na področju varnosti in drugih ustreznih programih Obzorja 2020.***

Predlog spremembe 78

Predlog direktive
Člen 8 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. V okviru mreže za sodelovanje ***pristojni organi***:	3. V okviru mreže za sodelovanje ***enotne kontaktne točke***:
(a) širijo zgodnja opozorila o tveganjih in incidentih v skladu s členom 10;	(a) širijo zgodnja opozorila o tveganjih in incidentih v skladu s členom 10;
(b) zagotavljajo usklajen odziv v skladu s členom 11;	(b) zagotavljajo usklajen odziv v skladu s členom 11;
(c) na skupnem spletišču redno objavljajo nezaupne informacije o tekočih zgodnjih opozorilih in usklajenem odzivu;	(c) na skupnem spletišču redno objavljajo nezaupne informacije o tekočih zgodnjih opozorilih in usklajenem odzivu;
(d) ***na zahtevo ene države članice ali Komisije*** v okviru področja uporabe te direktive skupaj ocenijo in razpravljajo o eni ali več nacionalnih strategijah in nacionalnih načrtih za sodelovanje na področju VOI iz člena 5;	(d) v okviru področja uporabe te direktive skupaj ocenijo in razpravljajo o eni ali več nacionalnih strategijah in nacionalnih načrtih za sodelovanje na področju VOI iz člena 5;
(e) ***na zahtevo države članice ali Komisije*** skupaj ocenijo in razpravljajo o učinkovitosti CERT, zlasti kadar vaje na področju VOI potekajo na ravni Unije;	(e) skupaj ocenijo in razpravljajo o učinkovitosti ***skupin*** CERT, zlasti kadar vaje na področju VOI potekajo na ravni Unije;
(f) sodelujejo z Europolovim centrom za kibernetsko kriminaliteto in drugimi ustreznimi evropskimi organi ter si z njimi izmenjujejo ***informacije o vseh*** pomembnih zadevah, zlasti na področju energije, prometa, bančništva, ***borze*** in zdravja;	(f) sodelujejo z Europolovim centrom za kibernetsko kriminaliteto in drugimi ustreznimi evropskimi organi ter si z njimi izmenjujejo ***znanje o*** pomembnih zadevah ***v zvezi z varnostjo omrežij in informacij***, zlasti na področju ***varstva podatkov,*** energije, prometa, bančništva, ***finančnih trgov*** in zdravja;
	(fa) kjer je ustrezno v obliki poročila obvestijo koordinatorja za boj proti terorizmu in lahko zaprosijo za pomoč pri analizi, pripravljalnemu delu in ukrepih mreže za sodelovanje;
(g) med seboj in s Komisijo izmenjujejo informacije in najboljše prakse ter si pomagajo pri gradnji zmogljivosti na področju VOI;	(g) med seboj in s Komisijo izmenjujejo informacije in najboljše prakse ter si pomagajo pri gradnji zmogljivosti na področju VOI;
(h) organizirajo redne medsebojne preglede o zmogljivostih in pripravljenosti;	
(i) organizirajo vaje na področju VOI na ravni Unije in po potrebi sodelujejo v	(i) organizirajo vaje na področju VOI na ravni Unije in po potrebi sodelujejo v

mednarodnih vajah na področju VOI.	mednarodnih vajah na področju VOI.
	(ia) vključujejo tržne udeležence, se z njimi posvetujejo ter, kjer je ustrezno, z njimi izmenjujejo informacije v zvezi s tveganji in incidenti, ki vplivajo na njihovo omrežje in informacijske sisteme;
	(ib) z namenom skupne razlage, skladne uporabe in doslednega izvajanja v Uniji v sodelovanju z agencijo ENISA razvijejo smernice za specifična sektorska merila za priglasitev večjih incidentov, ki dopolnijo parametre iz člena 14(2).

Predlog spremembe 79

Predlog direktive
Člen 8 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Mreža za sodelovanje enkrat letno objavi poročilo, ki temelji na dejavnostih mreže in na zbirnem poročilu, ki se predloži v skladu s členom 14(4) te direktive za preteklih 12 mesecev.

Predlog spremembe 80

Predlog direktive
Člen 8 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Komisija z izvedbenimi akti določi potrebne načine za lažje sodelovanje med ***pristojnimi organi in Komisijo*** iz odstavkov 2 in 3. Te izvedbene akte sprejme v skladu s postopkom ***posvetovanja*** iz člena 19(***2***).	4. Komisija z izvedbenimi akti določi potrebne načine za lažje sodelovanje med ***enotnimi kontaktnimi točkami, Komisijo in agencijo ENISA*** iz odstavkov 2 in 3. Te izvedbene akte sprejme v skladu s postopkom ***pregleda*** iz člena 19(***3***).

Predlog spremembe 81

Predlog direktive
Člen 9 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Udeleženci varne infrastrukture med drugim v vseh korakih obdelave izpolnjujejo ustrezne zahteve v zvezi z zaupnostjo in varnostne ukrepe v skladu z Direktivo 95/46/ES in Uredbo (ES) št. 45/2001.

Predlog spremembe 82

Predlog direktive
Člen 9 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Komisija se v skladu s členom 18 pooblasti za sprejemanje delegiranih aktov v zvezi z opredelitvijo meril, ki morajo biti izpolnjena, da država članica lahko sodeluje v sistemu za varno izmenjavo informacij, in sicer o:	***črtano***
(a) razpoložljivosti varne in odporne komunikacijske in informacijske infrastrukture na nacionalni ravni, ki je združljiva in interoperabilna z varno infrastrukturo mreže za sodelovanje v skladu s členom 7(3), in	
(b) ustreznih tehničnih, finančnih in človeških virih ter postopkih za pristojne organe in CERT, ki omogočajo uspešno, učinkovito in varno sodelovanje v sistemu za varno izmenjavo informacij po členih 6(3), 7(2) in 7(3).	

Predlog spremembe 83

Predlog direktive
Člen 9 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Komisija ***v skladu z merili iz odstavkov 2 in 3 z izvedbenimi*** akti sprejme ***sklepe o***	3. Komisija ***z delegiranimi*** akti sprejme ***skupen niz standardov o medsebojnem***

dostopu države članice do te varne infrastrukture. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).	***povezovanju in varnosti, ki jih morajo enotne kontaktne točke izpolniti pred izmenjavo občutljivih in zaupnih informacij znotraj mreže za sodelovanje.***

Predlog spremembe 84

Predlog direktive
Člen 10 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. ***Pristojni organi*** ali Komisija v mreži za sodelovanje izdajo zgodnja opozorila pri tveganjih in incidentih, ki izpolnjujejo vsaj enega od naslednjih pogojev:	1. ***Enotne kontaktne točke*** ali Komisija v mreži za sodelovanje izdajo zgodnja opozorila pri tveganjih in incidentih, ki izpolnjujejo vsaj enega od naslednjih pogojev:
(a) njihov obseg se hitro povečuje ali se lahko hitro poveča	
(b) ***presegajo ali lahko presežejo*** nacionalne zmogljivosti za odzivanje;	(b) ***enotna kontaktna točka oceni, da tveganje ali incident potencialno presega*** nacionalne zmogljivosti za odzivanje;
(c) ***vplivajo ali lahko vplivajo*** na več kot eno državo članico.	(c) ***enotne kontaktne točke ali Komisija ocenijo, da tveganje ali incident vpliva*** na več kot eno državo članico.

Predlog spremembe 85

Predlog direktive
Člen 10 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. V zgodnjih opozorilih ***pristojni organi*** in Komisija sporočijo vse razpoložljive pomembne informacije, ki bi bile lahko koristne za ocenjevanje tveganja ali incidentov.	2. V zgodnjih opozorilih ***enotne kontaktne točke*** in Komisija ***brez nepotrebnega odlašanja*** sporočijo vse razpoložljive pomembne informacije, ki bi bile lahko koristne za ocenjevanje tveganja ali incidentov.

Predlog spremembe 86

Predlog direktive
Člen 10 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Na zahtevo države članice ali na lastno pobudo lahko Komisija od države članice zahteva, da zagotovi vse ustrezne informacije o določenem tveganju ali incidentu.	***črtano***

Predlog spremembe 87

Predlog direktive
Člen 10 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi, da je kriminalne narave, ***pristojni organi ali Komisija*** o tem ***obvestijo*** Europolov center za kibernetsko kriminaliteto.	4. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi, da je kriminalne narave, ***in kadar zadevni tržni udeleženec v skladu s členom 15(4) poroča o incidentih, za katere sumi, da so resne kriminalne narave, države članice zagotovijo, da je*** o tem ***po potrebi obveščen*** Europolov center za kibernetsko kriminaliteto.

Predlog spremembe 88

Predlog direktive
Člen 10 – odstavek 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4a. Člani mreže za sodelovanje ne objavijo nobenih informacij o tveganjih in incidentih, ki jih prejmejo v skladu z odstavkom 1, ne da bi to predhodno odobrila enotna kontaktna točka, ki je informacije priglasila.
	Poleg tega enotna kontaktna točka, ki je informacije priglasila, pred izmenjavo informacij v mreži za sodelovanje o svoji

	nameri obvesti tržnega udeleženca, na katerega se informacije nanašajo, in če meni, da je ustrezno, zagotovi anonimnost zadevnih informacij.

Predlog spremembe 89

Predlog direktive
Člen 10 – odstavek 4 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4b. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi, da je resne tehnične narave na čezmejni ravni, enotne kontaktne točke ali Komisija o tem obvestijo agencijo ENISA;

Predlog spremembe 90

Predlog direktive
Člen 11 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Po zgodnjem opozarjanju iz člena 10 ***pristojni organi*** ocenijo ustrezne informacije in se nato dogovorijo o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI iz člena 12.	1. Po zgodnjem opozarjanju iz člena 10 ***enotne kontaktne točke*** ocenijo ustrezne informacije in se nato ***kar najhitreje*** dogovorijo o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI iz člena 12.

Predlog spremembe 91

Predlog direktive
Člen 12 – odstavek 2 – točka a – alinea 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– opredelitev oblike in postopkov za zbiranje in izmenjavo združljivih in primerljivih informacij o tveganjih in incidentih s strani ***pristojnih organov***,	– opredelitev oblike in postopkov za zbiranje in izmenjavo združljivih in primerljivih informacij o tveganjih in incidentih s strani ***enotnih kontaktnih točk***,

Predlog spremembe 92

Predlog direktive
Člen 12 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Načrt za sodelovanje Unije na področju VOI se sprejme najpozneje eno leto po začetku veljavnosti te direktive in se redno pregleduje.	3. Načrt za sodelovanje Unije na področju VOI se sprejme najpozneje eno leto po začetku veljavnosti te direktive in se redno pregleduje. ***Rezultati vsakega pregleda se sporočijo Evropskemu parlamentu.***

Predlog spremembe 93

Predlog direktive
Člen 12 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. V skladu s členom 5 te direktive se zagotovi skladnost med načrtom za sodelovanje Unije na področju VOI ter nacionalnimi strategijami in načrti za sodelovanje na področju VOI.

Predlog spremembe 94

Predlog direktive
Člen 13 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. V takih sporazumih se upošteva potreba po zagotavljanju ustreznega varstva osebnih podatkov v	Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. V takih sporazumih se upošteva potreba po zagotavljanju ustreznega varstva osebnih podatkov v

mreži za sodelovanje.	mreži za sodelovanje ***in določi postopek spremljanja, ki ga je treba uporabiti za zagotavljanje zaščite teh osebnih podatkov***. ***O pogajanjih o sporazumu se obvesti Evropski parlament. Vsak prenos osebnih podatkov prejemnikom v državah zunaj Unije se izvede v skladu s členoma 25 in 26 Direktive 95/46/ES in členom 9 Uredbe (ES) št. 45/2001.***

Predlog spremembe 95

Predlog direktive
Člen 13 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 13a
	Stopnja kritičnosti tržnih udeležencev
	Države članice lahko določijo raven kritičnosti tržnih udeležencev in pri tem upoštevajo posebnosti sektorjev, parametre, med drugim o pomenu posameznega tržnega udeleženca za vzdrževanje zadostne ravni sektorskih storitev, število strani, ki jim tržni udeleženec zagotavlja storitve, in obdobje, dokler prekinitev glavnih storitev tržnega udeleženca negativno vpliva na vzdrževanje ključnih gospodarskih in družbenih dejavnosti.

Obrazložitev

Ta predlog spremembe je del poglavja IV in bi moral biti pred spodnjim členom 14. Namen tega člena je bolj diferencirana razvrstitev v Prilogi II in posledično tudi obveznosti iz poglavja IV. Incidente morajo priglasiti vsi tržni udeleženci, ne glede na njihovo raven kritičnosti, pregled varnosti pa se lahko prilagodi stopnji kritičnosti tržnega udeleženca.

Predlog spremembe 96

Predlog direktive
Člen 14 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci sprejmejo ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju trenutnega tehnološkega stanja ti ukrepi zagotovijo raven varnosti, primerno zadevnemu tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev in zmanjšanje vpliva incidentov na ***ključne storitve*** omrežij in informacijskih sistemov, s čimer se zagotovi neprekinjenost storitev, ki jih podpirajo navedena omrežja in informacijski sistemi.	1. Države članice zagotovijo, da tržni udeleženci sprejmejo ustrezne ***in sorazmerne*** tehnične in organizacijske ukrepe za ***odkrivanje in učinkovito*** obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju trenutnega tehnološkega stanja ti ukrepi zagotovijo raven varnosti, primerno zadevnemu tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev in zmanjšanje vpliva incidentov na ***varnost ključnih storitev*** omrežij in informacijskih sistemov, s čimer se zagotovi neprekinjenost storitev, ki jih podpirajo navedena omrežja in informacijski sistemi.

Predlog spremembe 97

Predlog direktive
Člen 14 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci pristojnemu organu priglasijo incidente z bistvenim vplivom na ***varnost*** ključnih storitev, ki jih zagotavljajo.	2. Države članice zagotovijo, da tržni udeleženci pristojnemu organu ***ali enotni kontaktni točki brez nepotrebnega odlašanja*** priglasijo incidente z bistvenim vplivom na ***neprekinjenost*** ključnih storitev, ki jih zagotavljajo. ***Priglasitelj zaradi priglasitve ne nosi dodatne odgovornosti.*** ***Za določitev bistvenosti vpliva incidenta se med drugim upoštevajo naslednji parametri:***

Predlog spremembe 98

Predlog direktive
Člen 14 – odstavek 2 – točka a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(a) število uporabnikov, katerih ključna storitev je prizadeta;

Predlog spremembe 99

Predlog direktive
Člen 14 – odstavek 2 – točka b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(b) trajanje incidenta;

Predlog spremembe 100

Predlog direktive
Člen 14 – odstavek 2 – točka c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(c) geografska razširjenost, kar zadeva območje, ki ga je prizadel incident.

Predlog spremembe 101

Predlog direktive
Člen 14 – odstavek 2 – pododstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Ti parametri se podrobneje določijo v skladu s točko (ib) člena 8(3).

Predlog spremembe 102

Predlog direktive
Člen 14 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Tržni udeleženci priglasijo incident iz odstavkov 1 in 2 pristojnemu organu ali

enotni kontaktni točki v državi članici, v kateri je prizadeta ključna storitev. Če so prizadete ključne storitve v več državah članicah, enotna kontaktna točka, ki je prejela priglasitev, na podlagi informacij, ki jih posreduje tržni udeleženec, opozori druge zadevne enotne kontaktne točke. Tržni udeleženec bo v najkrajšem možnem času obveščen o tem, katere druge enotne kontaktne točke so bile obveščene o incidentu, ter tudi o sprejetih ukrepih, rezultatih ali drugih pomembnih informacijah o incidentu.

Predlog spremembe 103

Predlog direktive
Člen 14 – odstavek 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. Kadar priglasitev vsebuje osebne podatke, so ti dostopni le prejemnikom v okviru obveščenega pristojnega organa ali enotne kontaktne točke, ki morajo te podatke obdelati za opravljanje svojih nalog v skladu s pravili o zaščiti podatkov. Razkriti podatki so omejeni na to, kar je nujno za opravljanje njihovih nalog.

Predlog spremembe 104

Predlog direktive
Člen 14 – odstavek 2 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2c. Tržni udeleženci, ki jih Priloga II ne opredeljuje, lahko incidente prijavljajo prostovoljno po postopku iz člena 14(2).

Predlog spremembe 105

Predlog direktive
Člen 14 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. ***Pristojni organ*** lahko ***o incidentu*** obvesti javnost ***ali to zahteva od javnih uprav in tržnih udeležencev***, če ugotovi, da je ***razkritje incidenta v javnem interesu. Nacionalni pristojni organ enkrat na leto mreži za sodelovanje predloži kratko poročilo o prejetih priglasitvah in ukrepih, sprejetih v skladu*** s tem ***odstavkom***.	4. ***Po posvetovanju z obveščenim pristojnim organom in zadevnim tržnim udeležencem*** lahko ***enotna kontaktna točka*** obvesti javnost ***o posameznih incidentih***, če ugotovi, da je ***potrebna ozaveščenost javnosti, da se incident prepreči ali obravnava še trajajoči incident ali če je tržni udeleženec, ki je izpostavljen incidentu, zavrnil obravnavanje hude strukturne ranljivosti, povezane*** s tem ***incidentom, brez nepotrebnega odlašanja***. ***Pred javnim razkritjem pristojni organ, ki je informacije priglasil, zagotovi, da lahko tržni udeleženec pojasni svoje stališče in da je odločitev o javnem razkritju ustrezno usklajena z javnim interesom.*** ***Ob razkritju informacij o posameznih incidentih obveščeni pristojni organ ali enotna kontaktna točka poskrbi za kar največjo anonimnost.*** ***Če je to razumno mogoče, obveščeni pristojni organ ali enotna kontaktna točka zadevnemu tržnemu udeležencu zagotovi informacije, ki pripomorejo k učinkoviti obravnavi priglašenega incidenta.***
Nacionalni pristojni organ enkrat na leto ***mreži za sodelovanje*** predloži ***kratko*** poročilo o prejetih priglasitvah in ukrepih, sprejetih v skladu s tem odstavkom.	***Enotna kontaktna točka mreži za sodelovanje*** enkrat na leto predloži ***zbirno*** poročilo o prejetih priglasitvah***, vključno s številom priglasitev*** in ***parametri incidenta, ter o*** ukrepih, sprejetih v skladu s tem odstavkom.

Predlog spremembe 106

Predlog direktive
Člen 14 – odstavek 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4a. Države članice tržne udeležence spodbujajo, naj v svojih finančnih

	poročilih prostovoljno razkrijejo informacije o incidentih, v katere so vpletena njihova podjetja.

Predlog spremembe 107

Predlog direktive
Člen 14 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Komisija se v skladu s členom 18 pooblasti za sprejemanje delegiranih aktov v zvezi z opredelitvijo okoliščin, v katerih morajo javne uprave in tržni udeleženci priglasiti incidente.	***črtano***

Predlog spremembe 108

Predlog direktive
Člen 14 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. ***Ob upoštevanju delegiranih aktov, sprejetih v skladu z odstavkom 5, lahko*** pristojni organi sprejmejo smernice ***in po potrebi izdajo navodila*** glede okoliščin, v katerih morajo ***javne uprave in*** tržni udeleženci priglasiti incidente.	6. Pristojni organi ***ali enotne kontaktne točke lahko*** sprejmejo smernice glede okoliščin, v katerih morajo tržni udeleženci priglasiti incidente.

Predlog spremembe 109

Predlog direktive
Člen 14 – odstavek 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
8. Odstavka 1 in 2 se ne uporabljata za mikropodjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij[35].	8. Odstavka 1 in 2 se ne uporabljata za mikropodjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij[35]***, razen če mikropodjetje deluje kot hčerinsko podjetje tržnega udeleženca, kot je***

	opredeljeno v točki (b) člena 3(8).
[35] UL L 124, 20.5.2003, str. 36.	[35] UL L 124, 20.5.2003, str. 36.

Predlog spremembe 110

Predlog direktive
Člen 14 – odstavek 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	8a. Države članice se lahko odločijo, da bodo ta člen in člen 15 smiselno uporabljale za javne uprave.

Predlog spremembe 111

Predlog direktive
Člen 15 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice zagotovijo, da imajo pristojni organi ***vsa*** pooblastila, ***potrebna za preiskavo primerov, v katerih javne uprave ali*** tržni udeleženci ***ne*** izpolnjujejo obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.	1. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke ustrezna*** pooblastila, ***s katerimi zagotovijo, da*** tržni udeleženci izpolnjujejo obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.

Predlog spremembe 112

Predlog direktive
Člen 15 – odstavek 2 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Države članice zagotovijo, da imajo pristojni organi pooblastila, da od tržnih udeležencev ***in javnih uprav*** zahtevajo, da:	2. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** pooblastila, da od tržnih udeležencev zahtevajo, da:

Predlog spremembe 113

Predlog direktive
Člen 15 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) ***se zanje opravi pregled*** varnosti, ki ga izvede usposobljen neodvisen organ ali nacionalni organ, ter ***da se rezultati pregleda zagotovijo*** pristojnemu organu.	(b) ***zagotovijo dokaze o učinkovitem izvajanju varnostnih politik, na primer rezultate pregleda*** varnosti, ki ga izvede usposobljen neodvisen organ ali nacionalni organ, ter ***dajo dokaze na voljo*** pristojnemu organu ***ali enotni kontaktni točki***.

Predlog spremembe 114

Predlog direktive
Člen 15 – odstavek 2 – pododstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Pri pošiljanju zahteve pristojni organi in enotne kontaktne točke navedejo namen zahteve in zadovoljivo opredelijo, katere informacije so potrebne.

Predlog spremembe 115

Predlog direktive
Člen 15 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Države članice zagotovijo, da imajo pristojni organi pooblastila za izdajanje zavezujočih navodil za tržne udeležence ***in javne uprave***.	3. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** pooblastila za izdajanje zavezujočih navodil za tržne udeležence.

Predlog spremembe 116

Predlog direktive
Člen 15 – odstavek 3 a in 3 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Z odstopanjem od točke (b) odstavka 2 tega člena se lahko države članice odločijo, da morajo pristojni organi ali enotna kontaktna točka, kakor je primerno, za nekatere tržne udeležence uporabljati drug postopek, odvisno od njihove ravni kritičnosti, določene v skladu s členom 13a. Če se tako odločijo:
	(a) imajo pristojni organi ali enotna kontaktna točka, kakor je primerno, pooblastilo, da tržnim udeležencem predložijo dovolj specifično zahtevo, da zagotovijo dokaze o uspešnem izvajanju varnostnih politik, na primer rezultate pregleda varnosti, ki ga izvedejo notranji revizorji, in da dajo dokaze na voljo pristojnemu organu ali enotni kontaktni točki;
	(b) lahko pristojni organ ali enotna kontaktna točka potem, ko tržni udeleženec predloži zahtevo iz točke (a), po potrebi zahteva dodatne dokaze ali pregled, ki ga izvede usposobljen neodvisen organ ali nacionalni organ.
	3b. Države članice se lahko odločijo, da bodo za določenega tržnega udeleženca zmanjšale število in pogostost pregledov, če njihov pregled varnosti dosledno kaže skladnost s poglavjem IV.

Predlog spremembe 117

Predlog direktive
Člen 15 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Pristojni organi ***incidente***, za katere sumijo, da so kriminalne narave, ***priglasijo*** organom kazenskega pregona.	4. Pristojni organi ***in enotne kontaktne točke zadevne tržne udeležence obvestijo o tem***, ***da lahko o incidentih,*** za katere sumijo, da so ***resne*** kriminalne narave, ***poročajo*** organom kazenskega pregona.

Predlog spremembe 118

Predlog direktive
Člen 15 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi pri obravnavanju incidentov, katerih posledica je kršitev ***varstva*** osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov.	5. ***Brez poseganja v veljavna pravila o varstvu podatkov*** pristojni organi ***in enotne kontaktne točke*** pri obravnavanju incidentov, katerih posledica je kršitev ***varnosti*** osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov. ***Enotne kontaktne točke in organi za varstvo podatkov v sodelovanju z agencijo ENISA oblikujejo mehanizme za izmenjavo informacij in enotno predlogo, ki se uporablja za priglasitve v skladu s členom 14(2) te direktive in drugo zakonodajo Unije s področja zaščite podatkov.***

Predlog spremembe 119

Predlog direktive
Člen 15 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Države članice zagotovijo, da so obveznosti, ki se ***javnim upravam in*** tržnim udeležencem naložijo s tem poglavjem, lahko predmet sodne presoje.	6. Države članice zagotovijo, da so obveznosti, ki se tržnim udeležencem naložijo s tem poglavjem, lahko predmet sodne presoje.

Predlog spremembe 120

Predlog direktive
Člen 15 – odstavek 6 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	6a. Države članice se lahko odločijo, da bodo člen 14 in ta člen smiselno uporabljale za javne uprave.

Predlog spremembe 121

Predlog direktive
Člen 16 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Za zagotovitev usklajenega izvajanja člena 14(1) države članice spodbujajo uporabo standardov in/ali specifikacij, ki se nanašajo na varnost omrežij in informacij.	1. Za zagotovitev usklajenega izvajanja člena 14(1) države članice spodbujajo uporabo ***evropskih ali mednarodnih interoperabilnih*** standardov in/ali specifikacij, ki se nanašajo na varnost omrežij in informacij***, ne da bi predpisovale uporabo specifične tehnologije***.

Predlog spremembe 122

Predlog direktive
Člen 16 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Komisija z ***izvedbenimi akti*** pripravi seznam standardov, navedenih v odstavku 1. Seznam objavi v Uradnem listu Evropske unije.	2. Komisija ***ustreznemu evropskemu organu za standardizacijo podeli mandat, da po posvetovanju*** z ***ustreznimi zainteresiranimi stranmi*** pripravi seznam standardov ***in/ali specifikacij***, navedenih v odstavku 1. Seznam objavi v Uradnem listu Evropske unije.

Predlog spremembe 123

Predlog direktive
Člen 17 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Države članice zagotovijo, da se sankcije iz odstavka 1 tega člena uporabljajo samo, če tržni udeleženec namerno ali iz velike malomarnosti ni izpolnil svojih obveznosti iz poglavja IV.

Predlog spremembe 124

Predlog direktive
Člen 18 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Evropski parlament ali Svet lahko pooblastilo iz ***členov*** 9(2)***, 10(5) in 14(5)*** prekliče kadar koli. Z odločitvijo o preklicu preneha veljati prenos pooblastila, naveden v temu sklepu. Sklep začne učinkovati dan po objavi v Uradnem listu Evropske unije ali na poznejši datum, ki je v njem določen. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.	3. Evropski parlament ali Svet lahko pooblastilo iz ***člena*** 9(2) prekliče kadar koli. Z odločitvijo o preklicu preneha veljati prenos pooblastila, naveden v temu sklepu. Sklep začne učinkovati dan po objavi v Uradnem listu Evropske unije ali na poznejši datum, ki je v njem določen. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

Predlog spremembe 125

Predlog direktive
Člen 18 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Delegirani akt, sprejet v skladu s ***členi*** 9(2), ***10(5) in 14(5),*** začne veljati le, če Evropski parlament in Svet ne nasprotujeta delegiranemu aktu v dveh mesecih od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu**,** oziroma če ***sta*** 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.	5. Delegirani akt, sprejet v skladu s ***členom*** 9(2), začne veljati le, če Evropski parlament in Svet ne nasprotujeta delegiranemu aktu v dveh mesecih od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu oziroma 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 126

Predlog direktive
Člen 20 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Komisija redno pregleduje delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. Prvo poročilo	Komisija redno pregleduje delovanje te direktive***, predvsem seznam iz Priloge II,*** ter o tem poroča Evropskemu parlamentu

predloži najpozneje tri leta po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.	in Svetu. Prvo poročilo predloži najpozneje tri leta po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.

Predlog spremembe 127

Predlog direktive
Priloga 1 – naslov 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Zahteve in naloge ***skupine*** za odzivanje na računalniške grožnje (CERT)	Zahteve in naloge ***skupin*** za odzivanje na računalniške grožnje (CERT)

Predlog spremembe 128

Predlog direktive
Priloga 1 – odstavek 1 – točka 1 – odstavek a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) CERT zagotavljajo visoko razpoložljivost svojih komunikacijskih storitev tako, da preprečujejo posamezne točke okvar in vzpostavijo več kanalov, po katerih se drugi lahko ***obračajo*** nanje in one obrnejo na druge. Poleg tega se komunikacijski kanali jasno opredelijo ter jih uporabniki in partnerji dobro poznajo.	(a) ***Skupine*** CERT zagotavljajo visoko razpoložljivost svojih komunikacijskih storitev tako, da preprečujejo posamezne točke okvar in vzpostavijo več kanalov, po katerih se drugi lahko ***kadarkoli obrnejo*** nanje in one obrnejo na druge. Poleg tega se komunikacijski kanali jasno opredelijo ter jih uporabniki in partnerji dobro poznajo.

Predlog spremembe 129

Predlog direktive
Priloga 1 – odstavek 1 – točka 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) Uradi CERT in podporni informacijski sistemi se nahajajo na varnih krajih.	(c) Uradi ***skupin*** CERT in podporni informacijski sistemi se nahajajo na varnih krajih ***z zavarovanimi omrežnimi informacijskimi sistemi***.

Predlog spremembe 130

Predlog direktive
Priloga 1 – odstavek 1 – točka 2 – točka a – alinea 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– spremljanje incidentov na nacionalni ravni,	– ***odkrivanje in*** spremljanje incidentov na nacionalni ravni,

Predlog spremembe 131

Predlog direktive
Priloga 1 – odstavek 1 – točka 2 – točka a – alinea 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	– aktivno sodelovanje v evropskih in mednarodnih mrežah za sodelovanje CERT

Predlog spremembe 132

Predlog direktive
Priloga II – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Seznam tržnih udeležencev	Seznam tržnih udeležencev
Iz člena 3(8)a):	
1. Platforme za e-trgovanje	
2. Portali za spletna plačila	
3. Družabna omrežja	
4. Iskalniki	
5. Računalniške storitve v oblaku	
6. Prodajalne z aplikacijami	
Iz člena 3(8)b):	

Predlog spremembe 133

Predlog direktive
Priloga II – točka 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Seznam tržnih udeležencev	Seznam tržnih udeležencev
1. Energija	1. Energija
	(a) Električna energija
– Dobavitelji električne energije in plina	***– Dobavitelji***
– Upravljavci sistema distribucije električne energije in/ali plina ter dobavitelji za končne uporabnike	***– Upravljavci sistemov distribucije in dobavitelji za končne uporabnike***
– Upravljavci sistema za prenos zemeljskega plina, upravljavci skladišč in upravljavci obratov za UZP	
– Upravljavci sistema za prenos električne energije	***– Upravljavci sistema za prenos električne energije***
	(b) Nafta
– Upravljavci cevovodov za prenos nafte in skladiščenja nafte	***– Upravljavci cevovodov za prenos nafte in skladiščenje nafte***
	– Upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in prenosa nafte
	(c) Plin
– Udeleženci na trgu elektrike in plina	***– Dobavitelji***
	– Upravljavci sistemov distribucije in dobavitelji za končne uporabnike
	– Upravljavci sistemov za prenos zemeljskega plina, upravljavci sistemov za skladiščenje in upravljavci sistemov za UZP
– Upravljavci proizvodnje nafte in zemeljskega plina ter obratov za predelavo in rafiniranje	***– Upravljavci obratov za proizvodnjo, rafiniranje, predelavo in skladiščenje zemeljskega plina ter upravljavci prenosa zemeljskega plina***
	– Udeleženci na trgu plina

Predlog spremembe 134

Predlog direktive
Priloga II – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Promet	***2. Promet***
– Letalski prevozniki (tovorni in potniški zračni promet)	***(a) Cestni prevoz***
– Pomorski prevozniki (družbe za pomorski in obalni potniški promet in družbe za pomorski obalni tovorni promet)	***(i) Izvajalci nadzora upravljanja prometa***
– Železnice (upravitelji infrastrukture, integrirana podjetja in prevozniki v železniškem prometu)	***(ii) Pomožne logistične storitve:***
– Letališča	***– skladiščenje in shranjevanje,***
– Pristanišča	***– pretovarjanje in***
– Izvajalci nadzora upravljanja prometa	***– druge spremljajoče prevozne dejavnosti.***
– Pomožne logistične storitve: (a) skladiščenje in shranjevanje (b) ravnanje s tovorom in (c) druge spremljajoče prometne dejavnosti	***(b) Železniški prevoz***
	(i) Železnice (upravitelji infrastrukture, integrirana podjetja in prevozniki v železniškem prometu)
	(ii) Izvajalci nadzora upravljanja prometa
	(iii) Pomožne logistične storitve:
	– skladiščenje in shranjevanje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti.
	(c) Letalski promet
	(i) Letalski prevozniki (tovorni in potniški zračni promet)
	(ii) Letališča
	(iii) Izvajalci nadzora upravljanja prometa
	(iv) Pomožne logistične storitve:

	– skladiščenje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti.
	(d) Pomorski promet
	(i) Pomorski prevozniki (družbe za potniški promet po celinskih vodah ter pomorski in obalni potniški promet in družbe za tovorni promet po celinskih vodah ter pomorski in obalni tovorni promet)

Predlog spremembe 135

Predlog direktive
Priloga II – točka 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Infrastruktura finančnega trga: ***borze*** in klirinške hiše centralnih nasprotnih strank	4. Infrastruktura finančnega trga: ***organizirani trgi, večstranski sistemi trgovanja, sistemi organiziranega trgovanja*** in klirinške hiše centralnih nasprotnih strank

Predlog spremembe 136

Predlog direktive
Priloga II – točka 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Pridobivanje vode in preskrba z njo

Predlog spremembe 137

Predlog direktive
Priloga II – točka 5 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5b. Veriga preskrbe s hrano

Predlog spremembe 138

Predlog direktive
Priloga II – točka 5 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5c. Internetne izmenjevalne točke

OBRAZLOŽITEV

1. Ozadje

Digitalna agenda za Evropo je že leta 2010 pozivala k uvedbi zakonodajnih instrumentov, katerih cilj bi bila zagotovitev politike visoke ravni varnosti omrežij in informacij. Zaradi medsebojne prepletenosti omrežij in informacijskih sistemov lahko večje motnje enega od teh v eni državi članici prizadenejo drugo državo članico in Unijo kot celoto. Odpornost in trdnost omrežij in informacijskih sistemov pa tudi stalnost ključnih storitev so bistvene za nemoteno delovanje notranjega trga, še zlasti za nadaljnji razvoj enotnega digitalnega trga.

Glede na različne ravni zmogljivosti in razdrobljene pristope po Uniji je cilj Evropske komisije v sedanjem predlogu direktive o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji izboljšanje varnosti interneta ter zasebnih omrežij in informacijskih sistemov, ki podpirajo delovanje naše družbe in gospodarstva.

Zato Komisija od držav članic zahteva, da izboljšajo svojo pripravljenost ter medsebojno sodelovanje. V ta namen naj bi upravljavci ključne infrastrukture, kot so energija, promet ter ključni ponudniki storitev informacijske družbe, pa tudi javne uprave, sprejeli ustrezne ukrepe za obvladovanje varnostnih tveganj in resne incidente priglašali pristojnim nacionalnim organom.

2. Osnutek poročila

Poročevalec podpira splošni cilj predlagane direktive, tj. zagotavljanje visoke skupne ravni varnosti omrežij in informacij. Da bi okrepili učinkovitost predlaganih ukrepov, poročevalec meni, da bi morala biti ta direktiva v izhodišču omejena na določene upravljavce, varovati obstoječe naložbe v varnost omrežij in informacij ter se izogniti podvajanju institucionalnih struktur in obveznosti, ki se nalagajo tržnim udeležencem. Nadalje poročevalec meni, da bi morala ta direktiva podpirati razvoj odnosov, ki temeljijo na zaupanju, in izmenjav med javnimi in zasebnimi akterji ter da bi se bilo treba izogibati neželenim odzivom v obliki zgolj „kulture upoštevanja predpisov“ namesto želene „kulture obvladovanja tveganj“. Glede na te pomisleke poročevalec predlaga krepitev učinka te direktive z naslednjimi glavnimi spremembami.

A. Področje uporabe

Namen predloga direktive je nalaganje obveznosti javnim upravam in tržnim udeležencem, vključno s kritičnimi infrastrukturami in storitvami informacijske družbe. Da bi dosegli sorazmernost in hitre rezultate direktive, poročevalec meni, da bi bilo treba obvezne ukrepe iz poglavja IV omejiti na infrastrukture, ki so kritične v ožjem smislu. Po njegovem mnenju torej storitev informacijske družbe ne bi smeli vključiti v Prilogo II te direktive. Namesto tega bi se direktiva morala osredotočiti na tržne udeležence, ki zagotavljajo storitve, med drugim v

sektorjih energije in prometa ter na področju zdravja in infrastrukture finančnega trga.

Ob upoštevanju svojega javnega poslanstva morajo javne uprave posvečati potrebno skrbnost upravljanju lastnih omrežij in informacijskih sistemov. Zato poročevalec meni, da ni sorazmerno nalagati jim enake obveznosti kot tržnim udeležencem.
Poleg sprememb področja uporabe poročevalec podpira neizčrpno naravo Priloge II in se strinja z rednimi pregledi te direktive tudi zaradi tehnološkega razvoja.

B. Pristojni nacionalni organi

Predlog direktive predvideva imenovanje enega pristojnega nacionalnega organa na državo članico, ki je odgovoren za spremljanje uporabe direktive. Poročevalec meni, da to ne upošteva v zadostni meri že obstoječih struktur.
V nekaterih sektorjih, ki so zajeti v področje uporabe te direktive, tržni udeleženci uradno ali neuradno že priglašajo določene incidente na področju varnosti omrežij in informacij regulativnim organom v svojih sektorjih. Ob upoštevanju neposredne povezave in tesne povezanosti s svojimi sektorji imajo ti organi poglobljen vpogled v nevarnosti in ranljivosti, značilne za svoj sektor, in so zato v edinstvenem položaju, da ocenijo učinek morebitnih ali aktualnih incidentov v svojem sektorju.

Razen obstoječih sektorskih naložb bodo morale nekatere države članice zaradi ustavne strukture ali zaradi drugih vidikov morda imenovati več kot en pristojni nacionalni organ. Zato poročevalec predlaga spremembo direktive, da se omogoči imenovanje več kot enega pristojnega organa na državo članico. Vendar pa bi morala zaradi zagotavljanja dosledne uporabe znotraj države članice in zato, da se omogoči učinkovito in racionalno sodelovanje na ravni Unije, vsaka država članica imenovati eno enotno kontaktno točko, odgovorno med drugim za udeležbo v mreži za sodelovanje iz člena 8 in pošiljanje zgodnjih opozoril v skladu s členom 10.

C. Mreža za sodelovanje

Z namenom krepitve dejavnosti v mreži za sodelovanje poročevalec meni, da bi v mreži morali razmisliti o povabilu tržnih udeležencev k sodelovanju, kjer je to potrebno. Poleg tega bi letno poročilo o dejavnostih mreže dalo dragocene informacije o napredku pri izmenjavi najboljših praks med državami članicami in razvoju priglasitev incidentov po Uniji.

D. Varnostne zahteve in priglasitev incidentov

Kot glavno novost predlog direktive uvaja obvezno priglasitev incidentov, ki imajo bistven vpliv na varnost ključnih storitev, s strani tržnih udeležencev. Zaradi pojasnitve obsega obveznosti in njihove vključitve v osnovni akt poročevalec predlaga zamenjavo delegiranih aktov iz člena 14(5) z jasnimi merili za določitev bistvenosti incidentov, ki jih je treba priglasiti. Glede na nameravano uskladitev z Direktivo 2009/140/ES bi kazalniki, podobni tistim iz tehničnih smernic agencije ENISA v zvezi s poročanjem o incidentih za Direktivo 2009/140/ES, pojasnili obseg in merila za priglasitev. Poleg tega poročevalec priporoča okrepitev varoval v zvezi z objavo informacij, povezanih z incidenti, in pojasnjuje uporabo

zakonodaje v primeru, da incident prizadene ključne storitve v več državah članicah, z namenom preprečiti nalaganje večkratnih ali nejasnih obveznosti priglasitve.

E. Izvajanje in izvrševanje

Poročevalec meni, da je zelo pomembno spodbujati kulturo obvladovanja tveganj in graditi na obstoječih prizadevanjih tržnih udeležencev. Glede na to meni, da so bistvenejši splošno sodelovanje in konkretni ukrepi tržnih udeležencev kot določena oblika zagotavljanja informacij o konkretnih dejavnostih na področju obvladovanja tveganja.

Zato je v kontekstu člena 15 treba omogočiti prožnost v zvezi z dokazovanjem skladnosti z varnostnimi zahtevami, ki se naložijo tržnim udeležencem. Treba bi bilo sprejemati tudi druge dokaze skladnosti, ki niso v obliki pregleda varnosti.

F. Sankcije

Čeprav poročevalec vidi potrebo po zagotovitvi sankcij za tržne udeležence, ki ne ravnajo v skladu s predpisi, da se okrepi učinkovitost te direktive, pa meni, da morebitne sankcije ne bi smele odvračati od priglasitve incidentov in imeti neželenih učinkov. Izogniti bi se bilo treba situaciji, ko je hitra priglasitev incidenta ogrožena zaradi tveganja sankcij, med drugim zgolj zaradi nespoštovanja postopkovnih zahtev. Zato poročevalec predlaga pojasnitev, da se v primeru, ko tržni udeleženec ni upošteval obveznosti iz poglavja IV, vendar ni ravnal naklepno ali malomarno, sankcije ne naložijo.

19.12.2013

MNENJE ODBORA ZA INDUSTRIJO, RAZISKAVE IN ENERGETIKO(*)

za Odbor za notranji trg in varstvo potrošnikov

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Pripravljavka mnenja(*): Pilar del Castillo Vera

(*) Pridruženi odbor – člen 50 Poslovnika

KRATKA OBRAZLOŽITEV

Po pozivu Evropskega parlamenta v samoiniciativnem poročilu o digitalni agendi za Evropo je februarja 2013 Evropska komisija predstavila predlog direktive v zvezi z ukrepi, ki bi zagotovili visoko skupno raven varnosti omrežij in informacij v Uniji, in prvo strategijo EU za kibernetsko varnost. Pripravljavka mnenja pozdravlja predlog, saj z analizo razpoložljivih podatkov lahko ocenimo, da zlonamerni incidenti, povezani z IKT, lahko samo malim in srednjim podjetjem povzročijo za več kot 560 milijonov EUR neposrednih stroškov letno in da vse vrste incidentov (vključno z okoljskimi ali fizikalnimi problemi, kot so naravne katastrofe) lahko povzročijo za več kot 2,3 milijarde neposrednih stroškov.

Strukturno gledano se pripravljavka mnenja strinja s številnimi predlaganimi ukrepi, kot je razširitev določb v zvezi s poročanjem o varnostnih incidentih na druge sektorje kritične infrastrukture, saj je v skladu s členom 13a okvirne direktive iz leta 2009 poročanje omejeno zgolj na ponudnike telekomunikacijskih storitev. Predlogi, kot sta zahteva po ustrezno delujoči skupini za odzivanje na računalniške grožnje in določitev pristojnega organa, ki bi bil del vseevropskega omrežja za varno računalniško izmenjavo informacij in bi dopuščal varno izmenjavo informacij, povezanih s kibernetsko varnostjo, so zato dobro sprejeti, saj bi lahko znatno prispevali k cilju predlagane direktive, zlasti k zagotavljanju visoke skupne ravni varnosti omrežij in informacij v Uniji.

Pripravljavka mnenja vseeno meni, da je predlog možno še izboljšati, in sicer skozi prizmo dveh glavnih načel: učinkovitosti in zaupanja.

Prvo načelo – učinkovitost

V zvezi z obveznostjo držav članic, da morajo določiti pristojni organ za spremljanje uporabe

direktive v vseh sektorjih, navedenih v Prilogi II k predlogu, pripravljavka mnenja meni, da bi morala vsaka država članica imeti možnost izbrati zanjo najustreznejši model upravljanja kibernetske varnosti in da se je treba izogniti podvajanju institucionalnih struktur, ki bi lahko vodile do sporov glede pristojnosti in motenj v komunikaciji. Pripravljavka mnenja zato meni, da obstoječih nacionalnih struktur, ki so že uveljavljene in ki ustrezajo potrebam in ustavnim zahtevam držav članic, ne bi smeli spreminjati. Vseeno pa meni, da mora vsaka država članica za izmenjevanje informacij na ravni Unije, obveščanje o grožnjah v sistemu zgodnjega opozarjanja in uspešno sodelovanje v mreži za sodelovanje imenovati **enotno kontaktno točko**.

V istem duhu večanja učinkovitosti predlagane direktive pripravljavka mnenja meni, da predlagani ukrepi za vzpostavitev nacionalne **skupine za odzivanje na računalniške grožnje (CERT)** morda ne bodo najbolj primerni, saj ne upoštevajo drugačne narave in sestave obstoječih CERT. Ne samo, da ima večina držav članic več CERT, ampak se ti ukvarjajo z različnimi vrstami incidentov. Razlikujeta se tudi količina in kakovost dejavnosti, ki sta odvisni od tega, ali jih gostijo in upravljajo akademske ali raziskovalne institucije, vlada ali zasebni sektor. Poleg tega bi predlog prekinil obstoječe mednarodne in evropske mreže za sodelovanje, ki jim obstoječi CERT že pripadajo in ki so se izkazale za učinkovite pri usklajevanju mednarodnih in evropskih odzivov na incidente. Zato pripravljavka mnenja meni, da se direktiva ne sme nanašati na en nacionalni CERT, ampak se mora usmeriti k CERT, ki opravljajo storitve v sektorjih iz Priloge II, kar bi posledično pomenilo, da en CERT opravlja storitve v vseh sektorjih iz Priloge II ali da različni CERT opravljajo storitve v istem sektorju. Vseeno pa pripravljavka mnenja meni, da morajo države članice zagotoviti stalno polno operativnost CERT in ustrezne tehnične, finančne in človeške vire za uspešno delovanje in sodelovanje v mednarodnih in evropskih mrežah za sodelovanje.

Načelo učinkovitosti poleg tega zahteva spremembe predlagane direktive glede **področja uporabe**. Čeprav se pripravljavka mnenja strinja, da je treba razširiti obveznosti sistema za poročanje do energetskega, prometnega, zdravstvenega in finančnega sektorja, je predlog iz poglavja IV o razširitvi obveznih ukrepov na vse tržne udeležence v „internetnem gospodarstvu“ nesorazmeren in neobvladljiv. Nesorazmeren, ker je nekritična uvedba novih obveznosti do odprte in neopredeljene kategorije, kot je do vsakega „ponudnika storitev informacijske družbe, ki omogočajo zagotavljanje drugih storitev informacijske družbe“, ne samo nerazumljiva, ampak tudi neustrezno utemeljena glede na možno škodo, ki bi jo lahko povzročil varnostni incident, ter bi lahko povzročila dodatno birokracijo našemu industrijskemu sektorju, zlasti malim in srednjim podjetjem. Neobvladljiv, ker so se pojavili resni dvomi o zmožnosti pristojnih organov, da bi mogli vsa potencialna obvestila rešiti na proaktiven način, ki bi spodbujal dvosmerni dialog s tržnimi udeleženci v smeri reševanja varnostnih groženj.

V zvezi z **javno upravo** bi morala direktiva uravnotežiti potrebo po nadaljnjem razvoju storitev e-uprave in že obstoječe obveznosti skrbnega ravnanja, ki so naložene javni upravi in ki se dotikajo upravljanja in varovanja njihovih omrežij in informacijskih sistemov. Pripravljavka mnenja meni, da bi za javno upravo morale v celoti veljati zahteve po izmenjavi informacij iz člena 14, ne pa tudi obveznosti iz člena 15.

Drugo načelo – zaupanje

Po mnenju pripravljavke mnenja bo uspešnost direktive v veliki meri odvisna od tega, ali bodo tržni udeleženci pritegnjeni k sodelovanju in se bo vzpostavilo zaupanja vredno okolje varnosti omrežij in informacij, v katerem bodo pripravljeni proaktivno sodelovati. Če direktiva tega ne bo spodbudila, ne bo uspešna. V zvezi s tem pripravljavka mnenja predlaga, da je treba zagotoviti, da na udeležbo in obveščanje tržnih udeležencev ne bodo negativno vplivale nepotrebne objave prijavljenih varnostnih incidentov, in da tržni udeleženci niso odgovorni, če pristojni organi ali enotne kontaktne točke izgubijo informacije. Poleg tega mora med udeleženci in pristojnimi organi potekati dvosmerni dialog, sodelovanje tržnih udeležencev pa naj se spodbuja v vseh ustreznih forumih, tudi z mrežo za sodelovanje.

Pripravljavka mnenja še izraža prepričanje, da bi moralo biti zaupanje steber sodelovanja med pristojnimi odbori in/ali enotnimi kontaktnimi točkami, zlasti glede izmenjave informacij. Da bi to zagotovili, bi se morale določbe o zaupnosti in varnostih zahtevah omrežja odražati tudi v direktivi.

PREDLOGI SPREMEMB

Odbor za industrijo, raziskave in energetiko poziva Odbor za notranji trg in varstvo potrošnikov kot pristojni odbor, da v svoje poročilo vključi naslednje predloge sprememb:

Predlog spremembe 1

Predlog direktive
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga.	(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za ***svobodo in splošno varnost državljanov EU, za*** gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga.

Predlog spremembe 2

Predlog direktive
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Daljnosežnost ***in*** pogostnost ***namernih ali naključnih*** varnostnih incidentov se	(2) Daljnosežnost, pogostnost ***in učinek*** varnostnih incidentov se povečujeta in

povečujeta in pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo gospodarstvu Unije.	pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. ***Ti sistemi lahko prav tako postanejo lahka tarča za namerna škodljiva dejanja, namenjena povzročitvi škode ali prekinitvi delovanja sistemov.*** Takšni incidenti lahko ***ogrozijo zdravje in varnost prebivalstva***, ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov ***in vlagateljev*** in povzročijo veliko škodo gospodarstvu Unije.

Obrazložitev

Kibernetski napadi na podjetja, ki kotirajo na borzi, so zelo razširjeni (kraja finančnih sredstev in intelektualne lastnine teh podjetij, motnje v poslovanju njihovih strank ali poslovnih partnerjev) in lahko vplivajo na odnose z delničarji ter na odločitve potencialnih vlagateljev.

Predlog spremembe 3

Predlog direktive
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Kot komunikacijski instrument brez meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga.	(3) Kot komunikacijski instrument brez ***tradicionalnih*** meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev***, idej*** in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga, ***pa tudi za delovanje zunanjih trgov***.

Obrazložitev

Odpornost in stabilnost omrežij in informacijskih sistemov notranjega trga sta bistvenega pomena tudi za sodelovanje s svetovnimi in regionalnimi trgi, kot sta Severna Amerika ali Azija itd.

Predlog spremembe 4

Predlog direktive
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Na ravni Unije bi bilo treba vzpostaviti mehanizem za sodelovanje, ki bi omogočil izmenjavo informacij ter usklajeno odkrivanje in odzivanje na področju varnosti omrežij in informacij (VOI). Za učinkovito in vključujoče delovanje navedenega mehanizma je bistveno, da imajo vse države članice minimalne zmogljivosti in strategijo za zagotavljanje visoke ravni VOI na svojem ozemlju. Minimalne varnostne zahteve bi morale veljati tudi za javne ***uprave in*** upravljavce ***kritičnih*** informacijskih infrastruktur, da se spodbuja kultura obvladovanja tveganja in zagotovi poročanje o najresnejših incidentih.	(4) Na ravni Unije bi bilo treba vzpostaviti mehanizem za sodelovanje, ki bi omogočal izmenjavo informacij ter usklajeno ***preprečevanje,*** odkrivanje in odzivanje na področju varnosti omrežij in informacij (VOI). Za učinkovito in vključujoče delovanje navedenega mehanizma je bistveno, da imajo vse države članice minimalne zmogljivosti in strategijo za zagotavljanje visoke ravni VOI na svojem ozemlju. Minimalne varnostne zahteve bi morale veljati tudi za javne ***in zasebne*** upravljavce informacijskih infrastruktur ***in podjetja, ki kotirajo na borzi***, da se spodbuja kultura obvladovanja tveganja in zagotovi poročanje o najresnejših incidentih. ***Pravni okvir bi moral temeljiti na potrebi po varovanju zasebnosti in integritete državljanov. Informacijsko omrežje za opozarjanje o kritični infrastrukturi (CIWIN) bi bilo treba razširiti tudi na te upravljavce.***

Obrazložitev

Kršitve varnosti podjetij, ki kotirajo na borzi, bi lahko bistveno vplivale na izdelke in storitve teh podjetij ter njihove odnose s strankami ali dobavitelji in na splošne konkurenčne pogoje, s tem pa tudi na delovanje notranjega (in zunanjega) trga. Zato bi morala ta direktiva zajemati tudi podjetja, ki kotirajo na borzi.

Predlog spremembe 5

Predlog direktive
Uvodna izjava 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4a) Ta direktiva bi se morala osredotočati na kritično infrastrukturo, ki je bistvena za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energetike, prometa, bančništva, infrastrukture finančnega trga in zdravja.

Predlog spremembe 6

Predlog direktive
Uvodna izjava 4 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4b) Da vlade ne bi presegle ali zlorabile svojih pristojnosti, morajo biti informacijski in varnostni sistemi javnih organov pregledni, zakoniti, dobro zasnovani ter pregledno sprejeti z demokratičnim procesom.

Predlog spremembe 7

Predlog direktive
Uvodna izjava 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(6) Obstoječe zmogljivosti ne zadostujejo za zagotavljanje visoke ravni VOI v Uniji. Raven pripravljenosti v državah članicah je zelo različna, zato so tudi pristopi po Uniji razdrobljeni. Zaradi tega je raven varstva potrošnikov in podjetij neenaka, zmanjšuje pa se tudi skupna raven VOI v Uniji. Pomanjkanje skupnih minimalnih zahtev za ***javne uprave in*** tržne udeležence pa onemogoča vzpostavitev svetovnega in učinkovitega mehanizma za sodelovanje na ravni Unije.	(6) Obstoječe zmogljivosti ne zadostujejo za zagotavljanje visoke ravni VOI v Uniji. Raven pripravljenosti v državah članicah je zelo različna, zato so tudi pristopi po Uniji razdrobljeni. Zaradi tega je raven varstva potrošnikov in podjetij neenaka, zmanjšuje pa se tudi skupna raven VOI v Uniji. Pomanjkanje skupnih minimalnih zahtev za tržne udeležence pa onemogoča vzpostavitev svetovnega in učinkovitega mehanizma za sodelovanje na ravni Unije, ***kar še dodatno slabo vpliva na učinkovitost mednarodnega sodelovanja, s***

tem pa na boj proti svetovnim izzivom na področju varnosti, in spodkopava vodilni položaj Unije v mednarodnem merilu pri zagotavljanju in spodbujanju odprtega, učinkovitega in varnega interneta.

Predlog spremembe 8

Predlog direktive
Uvodna izjava 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) Za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov je zato potreben globalni pristop na ravni Unije, ki bi obsegal skupne minimalne zahteve za gradnjo zmogljivosti in njihovo načrtovanje, izmenjavo informacij in usklajevanje ukrepov ter minimalne varnostne zahteve ***za vse zadevne tržne udeležence in javne uprave***.	(7) Za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov je zato potreben globalni pristop na ravni Unije, ki bi obsegal skupne minimalne zahteve za gradnjo zmogljivosti in njihovo načrtovanje, ***razvoj zadostnih znanj na področju kibernetske varnosti,*** izmenjavo informacij in usklajevanje ukrepov ter skupne minimalne varnostne zahteve. ***Skupne minimalne standarde bi bilo treba uporabljati v skladu z ustreznimi priporočili usklajevalnih skupin za kibernetsko varnost (CSGC).***

Predlog spremembe 9

Predlog direktive
Uvodna izjava 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni, da bo	(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni ***na***

mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije.	***podlagi minimalnih zahtev iz te direktive***, da bo mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije. ***Zato bi morala vsaka država članica upoštevati skupne standarde v zvezi z obliko zapisa in možnostmi izmenjave podatkov, ki jih je treba izmenjevati in ocenjevati. Države članice lahko za pomoč pri oblikovanju nacionalnih strategij VOI na podlagi skupnega minimalnega načrta za strategijo VOI prosijo Evropsko agencijo za varnost omrežij in informacij (ENISA).***

Obrazložitev

Agencija ENISA pri ustreznih zainteresiranih straneh že uživa ugled visoko usposobljenega središča odličnosti in verodostojnega orodja za spodbujanje kibernetske varnosti v EU. Zato bi se morala EU izogibati podvajanju prizadevanj in struktur ter se opreti na strokovno znanje agencije ENISA in to agencijo zaprositi, naj prevzame svetovanje državam članicam, ki nimajo institucij VOI in strokovnega znanja.

Predlog spremembe 10

Predlog direktive
Uvodna izjava 10

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(10) Da se zagotovi učinkovito izvajanje določb, sprejetih v skladu s to direktivo, bi bilo treba v vsaki državi ustanoviti ali določiti organ za usklajevanje vprašanj VOI, ki bi deloval kot osrednja točka za čezmejno sodelovanje na ravni Unije. Ti organi bi morali imeti ustrezne tehnične, finančne in človeške vire, da bi lahko uspešno in učinkovito opravljali dodeljene naloge ter tako dosegli cilje te direktive.	(10) Da se zagotovi učinkovito izvajanje določb, sprejetih v skladu s to direktivo, bi bilo treba v vsaki državi članici ustanoviti ali določiti organ za usklajevanje vprašanj VOI, ki bi deloval kot ***enotna*** osrednja točka ***za notranje usklajevanje in*** čezmejno sodelovanje na ravni Unije. ***Te enotne nacionalne kontaktne točke bi bilo treba določiti brez poseganja v pravico držav članic, da v skladu z ustavnimi, sodnimi ali upravnimi zahtevami določijo več kot en nacionalni pristojni organ, ki bo zagotavljal varnost omrežij in informacij, vendar bi morale kljub temu biti pristojne za usklajevanje na***

nacionalni ravni in ravni Unije. Ti organi bi morali imeti ustrezne tehnične, finančne in človeške vire, da bi lahko ***neprekinjeno,*** uspešno in učinkovito opravljali dodeljene naloge ter tako dosegli cilje te direktive.

Predlog spremembe 11

Predlog direktive
Uvodna izjava 10 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(10a) Glede na razlike v nacionalnih strukturah upravljanja in da bi zavarovali obstoječe sektorske dogovore ter preprečili podvajanje, bi morale imeti države članice v okviru te direktive možnost imenovati več kot en nacionalni pristojni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov tržnih udeležencev. Za nemoteno čezmejno sodelovanje in komunikacije pa je nujno, da vsaka država članica imenuje samo eno nacionalno enotno kontaktno točko, odgovorno za čezmejno sodelovanje na ravni Unije. Če ustavna struktura ali druge ureditve tako zahtevajo, bi morala država članica imeti možnost imenovati samo en organ za izvajanje nalog pristojnega organa in enotne kontaktne točke.

Predlog spremembe 12

Predlog direktive
Uvodna izjava 11

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(11) Vse države članice bi morale imeti ustrezne tehnične in organizacijske zmogljivosti ***za preprečevanje, odkrivanje, odzivanje in ublažitev incidentov in tveganj VOI***. Zato bi bilo treba v vseh	(11) Vse države članice ***in tržni udeleženci*** bi morali imeti ustrezne tehnične in organizacijske zmogljivosti***, da kadar koli preprečijo, odkrijejo in ublažijo incidente in tveganja VOI ter se nanje odzovejo***.

državah članicah ustanoviti dobro delujoče skupine za odzivanje na računalniške grožnje, ki bi izpolnjevale bistvene zahteve, da se zagotovijo učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter učinkovito sodelovanje na ravni Unije.

Varnostni sistemi javnih uprav morajo biti varni in predmet demokratičnega nadzora in pregleda. Običajno potrebna oprema in zmogljivosti bi morale biti usklajene s skupno dogovorjenimi tehničnimi standardi in standardnimi operativnimi postopki. Zato bi bilo treba v vseh državah članicah ustanoviti dobro delujoče skupine za odzivanje na računalniške grožnje ***(CERT)***, ki bi izpolnjevale bistvene zahteve, da se zagotovijo učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter učinkovito sodelovanje na ravni Unije. ***Tem skupinam bi morali omogočiti sodelovanje na podlagi skupnih tehničnih standardov in standardnih operativnih postopkov. Glede na različne značilnosti obstoječih CERT, ki se odzivajo na različne tematske potrebe in akterje, bi morale države članice zagotoviti, da za vse sektorje iz Priloge II, storitve zagotavlja najmanj eden izmed njih. Glede čezmejnega sodelovanja skupin CERT bi morale države članice zagotoviti, da bodo imele na voljo dovolj sredstev za sodelovanje v obstoječih mednarodnih in evropskih mrežah sodelovanja.***

Obrazložitev

Zagotoviti je treba interoperabilnost.

Predlog spremembe 13

Predlog direktive
Uvodna izjava 12

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(12) Na podlagi znatnega napredka, doseženega v okviru evropskega foruma držav članic pri spodbujanju razprave in izmenjave dobrih praks, vključno s pripravo načel za sodelovanje v EU pri kibernetskih krizah, bi morale države članice in Komisija oblikovati mrežo, prek	(12) Na podlagi znatnega napredka, doseženega v okviru evropskega foruma držav članic pri spodbujanju razprave in izmenjave dobrih praks, vključno s pripravo načel za sodelovanje v EU pri kibernetskih krizah, bi morale države članice in Komisija oblikovati mrežo, prek

katere bi lahko stalno komunicirale in poglobile svoje sodelovanje. Ta varen in učinkovit mehanizem za sodelovanje bi moral omogočiti strukturirano in usklajeno izmenjavo informacij, odkrivanje in odzivanje na ravni Unije.	katere bi lahko stalno komunicirale in poglobile svoje sodelovanje. Ta varen in učinkovit mehanizem za sodelovanje ***– če bo zagotovljena udeležba tržnih udeležencev –*** bi moral omogočiti strukturirano in usklajeno izmenjavo informacij, odkrivanje in odzivanje na ravni Unije.

Predlog spremembe 14

Predlog direktive
Uvodna izjava 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(13) Evropska agencija za varnost omrežij in informacij (ENISA) bi morala državam članicam in Komisiji pomagati s strokovnim znanjem in svetovanjem ter spodbujati izmenjavo najboljših praks. Komisija bi se ***morala*** z ENISA posvetovati zlasti pri uporabi te direktive. Da se zagotovi učinkovito in pravočasno obveščanje držav članic in Komisije, bi bilo treba zgodnja opozorila o incidentih in tveganjih priglasiti v mreži za sodelovanje. Da se vzpostavijo zmogljivosti in znanje med državami članicami, bi morala mreža za sodelovanje služiti tudi kot orodje za izmenjavo najboljših praks ter z usmerjanjem organizacije medsebojnih pregledov in vaj na področju VOI članom pomagati pri gradnji zmogljivosti.	(13) Evropska agencija za varnost omrežij in informacij (ENISA) bi morala državam članicam in Komisiji pomagati s strokovnim znanjem in svetovanjem ter spodbujati izmenjavo najboljših praks. Komisija ***in države članice*** bi se ***morale*** z ENISA posvetovati zlasti pri uporabi te direktive. Da se zagotovi učinkovito in pravočasno obveščanje držav članic in Komisije, bi bilo treba zgodnja opozorila o incidentih in tveganjih priglasiti v mreži za sodelovanje. Da se vzpostavijo zmogljivosti in znanje med državami članicami, bi morala mreža za sodelovanje služiti tudi kot orodje za izmenjavo najboljših praks ter z usmerjanjem organizacije medsebojnih pregledov in vaj na področju VOI članom pomagati pri gradnji zmogljivosti.

Predlog spremembe 15

Predlog direktive
Uvodna izjava 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) ***Treba bi bilo*** vzpostaviti varno infrastrukturo za izmenjavo informacij, ki bi omogočila izmenjavo občutljivih in zaupnih informacij v okviru mreže za sodelovanje. Ne glede na obveznosti držav članic, da incidente in tveganja z evropsko razsežnostjo priglasijo v mreži za sodelovanje, bi moral biti dostop do zaupnih informacij iz drugih držav članic dovoljen samo, če države članice dokažejo, da njihovi tehnični, finančni in človeški viri ter postopki in komunikacijska infrastruktura zagotavljajo učinkovito, uspešno in varno sodelovanje v mreži.	(14) ***Pod nadzorom agencije ENISA bi bilo treba*** vzpostaviti varno infrastrukturo za izmenjavo informacij, ki bi omogočila izmenjavo občutljivih in zaupnih informacij v okviru mreže za sodelovanje. Ne glede na obveznosti držav članic, da incidente in tveganja z evropsko razsežnostjo priglasijo v mreži za sodelovanje, bi moral biti dostop do zaupnih informacij iz drugih držav članic dovoljen samo, če države članice dokažejo, da njihovi tehnični, finančni in človeški viri ter postopki in komunikacijska infrastruktura zagotavljajo učinkovito, uspešno in varno sodelovanje v mreži. ***Da bi lahko mreža za sodelovanje učinkovito izpolnila svojo nalogo, bi morala Komisija zanjo določiti proračunsko vrstico.***

Predlog spremembe 16

Predlog direktive
Uvodna izjava 14 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(14a) Po potrebi se lahko dejavnosti mreže za sodelovanje na povabilo udeležujejo tudi tržni udeleženci.

Predlog spremembe 17

Predlog direktive
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne	(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne

udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem ter si izmenjevati informacije in najboljše prakse v zameno za operativno podporo pri incidentih.

udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem ter si ***medsebojno*** izmenjevati informacije in najboljše prakse***, vključno z vzajemno izmenjavo ustreznih informacij,*** operativno podporo ***in strateško analiziranimi informacijami*** pri incidentih. ***Za uspešno spodbujanje izmenjave informacij in najboljših praks je treba zagotoviti, da tržni udeleženci, ki pri tem sodelujejo, zaradi tega ne bodo prikrajšani. Vzpostaviti je treba ustrezne zaščitne ukrepe, da udeleženci zaradi omenjenega sodelovanja ne bodo izpostavljeni večjim tveganjem glede skladnosti ali novih obveznosti, ki izhajajo iz zakonodaje na področju – med drugim – konkurence, intelektualne lastnine, varstva podatkov ali kibernetske kriminalitete, ali večjim operativnim ali varnostnim tveganjem.***

Predlog spremembe 18

Predlog direktive
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi ***morali pristojni organi*** vzpostaviti skupno spletišče, na katerem bi objavljali nezaupne informacije o incidentih ***in*** tveganjih.	(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi ***morale enotne kontaktne točke*** vzpostaviti skupno spletišče ***na ravni Unije***, na katerem bi objavljale nezaupne informacije o incidentih, tveganjih ***in načinih za zmanjšanje tveganj, po potrebi pa tudi svetovale o ustreznih vzdrževalnih ukrepih***.

Predlog spremembe 19

Predlog direktive
Uvodna izjava 17

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(17) Če se informacije štejejo za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, se pri izvajanju dejavnosti in izpolnjevanju ciljev te direktive zagotovi njihova zaupnost.	(17) ***Politika določanja stopenj tajnosti informacij iz uvodne izjave 14 bi se morala opirati na semaforni protokol za izmenjavo informacij, ki ga priporoča ENISA. Vse izmenjane informacije se razvrstijo in obravnavajo glede na stopnjo občutljivosti, ki jo določi vir informacij.*** Če se informacije štejejo za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, se pri izvajanju dejavnosti in izpolnjevanju ciljev te direktive zagotovi njihova zaupnost.

Predlog spremembe 20

Predlog direktive
Uvodna izjava 18

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(18) Komisija in države članice bi morale zlasti na podlagi nacionalnih izkušenj s področja kriznega upravljanja in v sodelovanju z agencijo ENISA pripraviti načrt za sodelovanje Unije na področju VOI, v katerem bi opredelile mehanizme za sodelovanje pri obvladovanju tveganj in incidentov. Ta načrt bi bilo treba ustrezno upoštevati pri zgodnjem opozarjanju v mreži za sodelovanje.	(18) Komisija in države članice bi morale zlasti na podlagi nacionalnih izkušenj s področja kriznega upravljanja in v sodelovanju z agencijo ENISA pripraviti načrt za sodelovanje Unije na področju VOI, v katerem bi opredelile mehanizme za sodelovanje, ***najboljše prakse in vzorce delovanja*** pri ***preprečevanju, odkrivanju, poročanju in*** obvladovanju tveganj in incidentov. Ta načrt bi bilo treba ustrezno upoštevati pri zgodnjem opozarjanju v mreži za sodelovanje.

Predlog spremembe 21

Predlog direktive
Uvodna izjava 19

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(19) Priglasitev zgodnjega opozarjanja v mreži bi bilo treba zahtevati le, kadar bi obseg in resnost incidenta ali zadevnega tveganja postala ali lahko postala tako pomembna, da bi bilo potrebno obveščanje ali usklajevanje odziva na ravni Unije. Zgodnje opozarjanje bi moralo biti zato omejeno na ***dejanske ali možne*** incidente ali tveganja, ki se hitro povečujejo, presegajo nacionalne zmogljivosti odzivanja ali prizadenejo več kot eno državo članico. Da se omogoči pravilna ocena, bi bilo treba vse informacije, ki so pomembne za oceno tveganja ali incidenta, priglasiti v mreži za sodelovanje.	(19) Priglasitev zgodnjega opozarjanja v mreži bi bilo treba zahtevati le, kadar bi obseg in resnost incidenta ali zadevnega tveganja postala ali lahko postala tako pomembna, da bi bilo potrebno obveščanje ali usklajevanje odziva na ravni Unije. Zgodnje opozarjanje bi moralo biti zato omejeno na incidente ali tveganja, ki se hitro povečujejo, presegajo nacionalne zmogljivosti odzivanja ali prizadenejo več kot eno državo članico. Da se omogoči pravilna ocena, bi bilo treba vse informacije, ki so pomembne za oceno tveganja ali incidenta, priglasiti v mreži za sodelovanje.

Predlog spremembe 22

Predlog direktive
Uvodna izjava 20

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(20) Ko ***pristojni organi*** prejmejo zgodnje opozorilo in njegovo oceno, bi se morali dogovoriti o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI. ***Pristojne organe*** in Komisijo bi bilo treba obvestiti o ukrepih, sprejetih na nacionalni ravni, ki so posledica usklajenega odziva.	(20) Ko ***enotne kontaktne točke*** prejmejo zgodnje opozorilo in njegovo oceno, bi se morale dogovoriti o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI. ***Enotne kontaktne točke*** in Komisijo bi bilo treba obvestiti o ukrepih, sprejetih na nacionalni ravni, ki so posledica usklajenega odziva.

Predlog spremembe 23

Predlog direktive
Uvodna izjava 22

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(22) Odgovornost za zagotavljanje VOI imajo v veliki meri javne uprave in tržni	(22) Odgovornost za zagotavljanje VOI imajo v veliki meri javne uprave in tržni

udeleženci. Kulturo obvladovanja tveganja, ki vključuje oceno tveganja in izvajanje ustreznih varnostnih ukrepov za zadevna tveganja, bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. Vzpostavitev enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.

udeleženci. Kulturo obvladovanja tveganja***, tesnega sodelovanja in zaupanja***, ki vključuje oceno tveganja in izvajanje ustreznih varnostnih ukrepov za zadevna tveganja, bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. Vzpostavitev ***zaupanja vrednih,*** enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.

Predlog spremembe 24

Predlog direktive
Uvodna izjava 24

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(24) Te obveznosti bi bilo treba razširiti prek sektorja elektronskih komunikacij, da bi veljale tudi za glavne ponudnike storitev informacijske družbe, kakor so opredeljeni v Direktivi 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov ter pravil o storitvah informacijske družbe[27], ki so podlaga za storitve informacijske družbe na podrejenem trgu ali spletne dejavnosti, kot so platforme za e-trgovanje, portali za spletna plačila, družabna omrežja, iskalniki, storitve računalništva v oblaku, prodajalne z aplikacijami. Prekinitve teh ***omogočitvenih storitev informacijske družbe ovirajo zagotavljanje drugih storitev informacijske družbe, ki so odvisne od njih***. ***Razvijalci programske opreme in proizvajalci strojne opreme niso ponudniki storitev informacijske družbe, zato za njih te obveznosti ne veljajo. Navedene obveznosti bi bilo treba razširiti tudi na javne uprave in upravljavce kritične infrastrukture, ki so***	(24) Te obveznosti bi bilo treba razširiti prek sektorja elektronskih komunikacij ***na upravljavce infrastrukture, ki so močno odvisni od informacijskih in komunikacijskih tehnologij ter so bistveni za vzdrževanje ključnih gospodarskih in družbenih funkcij, kot so električna energija in plin, promet, kreditne institucije, infrastruktura finančnega trga in zdravje***. Prekinitve teh ***omrežij in informacijskih sistemov bi negativno vplivale na notranji trg. Čeprav obveznosti iz te direktive ne veljajo*** za glavne ponudnike storitev informacijske družbe, kakor so opredeljeni v Direktivi 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov ter pravil o storitvah informacijske družbe[27], ki so podlaga za storitve informacijske družbe na podrejenem trgu ali spletne dejavnosti, kot so platforme za e-trgovanje, portali za spletna plačila, družabna omrežja, iskalniki, storitve računalništva v oblaku ***na splošno ali*** prodajalne z aplikacijami,

močno odvisni od informacijskih in komunikacijskih tehnologij ter so bistveni za vzdrževanje ključnih gospodarskih in družbenih funkcij, kot so električna energija in plin, promet, kreditne institucije, borze in zdravje. Prekinitve teh omrežij in informacijskih sistemov bi vplivale na notranji trg.	***pa lahko ti prostovoljno obvestijo pristojni organ ali enotno kontaktno točko o omrežnih varnostnih incidentih, za katere presodijo, da je to primerno, pristojni organ ali enotna kontaktna točka pa bi morala, če je to razumno mogoče, tržnim udeležencem, ki so sporočili incident, zagotoviti strateško analizirane informacije, ki jim bodo pomagale odpraviti varnostno grožnjo.***
[27] UL L 204, 21.7.1998, str. 37.	[27] UL L 204, 21.7.1998, str. 37.

Predlog spremembe 25

Predlog direktive
Uvodna izjava 25

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(25) Tehnični in organizacijski ukrepi za ***javne uprave in*** tržne udeležence ne bi smeli predpisovati, da se določen komercialni izdelek IKT oblikuje, razvije ali proizvede na določen način.	(25) Tehnični in organizacijski ukrepi za tržne udeležence ne bi smeli predpisovati, da se določen komercialni izdelek IKT oblikuje, razvije ali proizvede na določen način. ***Na drugi strani bi bilo treba zahtevati uporabo mednarodnih standardov v zvezi s kibernetsko varnostjo.***

Predlog spremembe 26

Predlog direktive
Uvodna izjava 28

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(28) Pristojni organi bi morali ustrezno pozornost nameniti ohranjanju neuradnih in zanesljivih kanalov za izmenjavo informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom, bi bilo treba najti ravnotežje med interesom	(28) Pristojni organi ***in enotne kontaktne točke*** bi morali ustrezno pozornost nameniti ohranjanju neuradnih in zanesljivih kanalov za izmenjavo informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. ***Pristojni organi bi morali proizvajalce in ponudnike prizadetih izdelkov in storitev***

javnosti, da je obveščena o nevarnostih, ter morebitno škodo za ugled in poslovanje ***javnih uprav in*** tržnih udeležencev, ki priglasijo incidente. Pri izvajanju obveznosti priglasitve bi morali pristojni organi posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne do ustreznega popravila varnosti.

IKT obvestiti o prej neznani ranljivosti ali incidentih, ki so bili priglašeni. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom ***in enotnim kontaktnim točkam***, bi bilo treba najti ravnotežje med interesom javnosti, da je obveščena o nevarnostih, ter morebitno škodo za ugled in poslovanje tržnih udeležencev, ki priglasijo incidente. ***Da bi ohranili zaupanje in učinkovitost, bi moralo obveščanje javnosti o incidentih potekati samo po posvetovanju s tistimi, ki so poročali o incidentu in le, kadar je to nujno potrebno za doseganje ciljev te direktive***. Pri izvajanju obveznosti priglasitve bi morali pristojni organi ***in enotne kontaktne točke*** posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne do ustreznega popravila varnosti, ***vendar ne bi smeli odlašali s priglasitvami dlje, kot je to obvezno***. ***Enotne kontaktne točke praviloma ne bi smele razkrivati osebnih podatkov posameznikov, vpletenih v incidente. Osebne podatke bi smele razkriti samo v primeru, da je njihovo razkritje nujno in sorazmerno glede na zastavljeni cilj.***

Obrazložitev

Če so bili organi seznanjeni z ranljivostjo določenih izdelkov ali storitev IKT, bi morali o tem obvestiti proizvajalce in ponudnike storitev, da bodo lahko pravočasno prilagodili svoje izdelke in storitve.

Predlog spremembe 27

Predlog direktive
Uvodna izjava 29

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(29) Pristojni organi bi morali imeti potrebna sredstva za opravljanje svojih nalog, vključno s pooblastili za pridobivanje zadostnih informacij od tržnih	(29) Pristojni organi ***in enotne kontaktne točke*** bi morali imeti potrebna sredstva za opravljanje svojih nalog, vključno s pooblastili za pridobivanje zadostnih

udeležencev in javnih uprav, da lahko ocenijo raven varnosti omrežij in informacijskih sistemov ter zanesljivih in izčrpnih podatkov o dejanskih incidentih, ki so vplivali na delovanje omrežij in informacijskih sistemov.

informacij od tržnih udeležencev in javnih uprav, da lahko ocenijo raven varnosti omrežij in informacijskih sistemov ***in izmerijo število in obseg incidentov*** ter zanesljivih in izčrpnih podatkov o dejanskih incidentih, ki so vplivali na delovanje omrežij in informacijskih sistemov.

Predlog spremembe 28

Predlog direktive
Uvodna izjava 30

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(30) V mnogih primerih so v ozadju incidentov kriminalne dejavnosti. Sum za to je možen tudi, če na začetku še niso dovolj jasnih dokazov. Pri tem bi moralo biti primerno sodelovanje med pristojnimi organi in organi pregona sestavni del učinkovitega in celovitega odzivanja na ogroženost zaradi varnostnih incidentov. Pri spodbujanju varnega in odpornejšega okolja je pomembno zlasti, da se incidenti, za katere obstaja sum, da so resne kriminalne narave, sistematično priglasijo organom kazenskega pregona. Resno kriminalno naravo incidentov bi bilo treba oceniti ob upoštevanju predpisov EU o kibernetski kriminaliteti.	(30) V mnogih primerih so v ozadju incidentov kriminalne dejavnosti ***ali dejavnosti kibernetske vojne***. Sum za to je možen tudi, če na začetku še niso dovolj jasnih dokazov. Pri tem bi moralo biti primerno sodelovanje med pristojnimi organi***, enotnimi kontaktnimi točkami*** in organi pregona ter ***sodelovanje z Europolovim centrom za kibernetsko kriminaliteto in agencijo ENISA*** sestavni del učinkovitega in celovitega odzivanja na ogroženost zaradi varnostnih incidentov. Pri spodbujanju varnega in odpornejšega okolja je pomembno zlasti, da se incidenti, za katere obstaja sum, da so resne kriminalne narave, sistematično priglasijo organom kazenskega pregona. Resno kriminalno naravo incidentov bi bilo treba oceniti ob upoštevanju predpisov EU o kibernetski kriminaliteti.

Predlog spremembe 29

Predlog direktive
Uvodna izjava 31

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(31) V številnih primerih je zaradi incidentov kršena varnost osebnih podatkov. Zato bi morali pristojni organi in organi za varstvo podatkov pri preprečevanju kršitev varnosti osebnih podatkov, nastalih zaradi incidentov, med seboj sodelovati in si izmenjevati pomembne informacije. Če varnostni incident pomeni tudi kršitev varstva osebnih podatkov ***v skladu z Uredbo Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov[28], države članice varnostne incidente priglasijo*** z najmanjšo možno upravno obremenitvijo. ENISA bi ***lahko sodelovala s pristojnimi organi in organi za varstvo podatkov ter pripravila*** mehanizme in ***predloge za izmenjavo informacij, s katerimi bi odpravila podvajanje obrazca za priglasitev***. ***En sam*** obrazec za priglasitev bi omogočil lažje poročanje o incidentih, ki se nanašajo na varstvo osebnih podatkov, s čimer bi se zmanjšala upravna obremenitev za podjetja in javne uprave.	(31) V številnih primerih je zaradi incidentov kršena varnost osebnih podatkov. ***Države članice in tržni udeleženci bi morali shranjene, obdelane ali poslane osebne podatke zaščititi pred nenamernim ali nezakonitim uničenjem, nenamerno izgubo ali spremembami in nepooblaščenimi ali nezakonitimi oblikami hrambe, dostopa, razkrivanja ali razširjanja in zagotoviti izvajanje varnostne politike v zvezi z obdelavo osebnih podatkov.*** Zato bi morali pristojni organi, ***enotne kontaktne točke*** in organi za varstvo podatkov pri preprečevanju kršitev varnosti osebnih podatkov, nastalih zaradi incidentov, med seboj sodelovati in si izmenjevati pomembne informacije. Če varnostni incident pomeni tudi kršitev varstva osebnih podatkov, ***ki jo je treba priglasiti v skladu z veljavnim pravom***, ***se obveznost priglasitve izvede*** z najmanjšo možno upravno obremenitvijo. ENISA bi ***morala pripraviti*** mehanizme za izmenjavo informacij in enoten obrazec za priglasitev***,*** ***ki*** bi omogočal lažje poročanje o incidentih, ki se nanašajo na varstvo osebnih podatkov, s čimer bi se zmanjšala upravna obremenitev za podjetja in javne uprave.

[28] SEC(2012) 72 final

Obrazložitev

Usklajeno z osnutkom direktive o varstvu podatkov.

Predlog spremembe 30

Predlog direktive
Uvodna izjava 32

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(32) Standardizacija varnostnih zahtev je tržno usmerjen proces. Da se zagotovi usklajena uporaba varnostnih standardov, bi morale države članice spodbujati uporabo in upoštevanje določenih standardov ter tako zagotoviti visoko raven varnosti na ravni Unije. Zato ***bi bilo morda treba pripraviti*** osnutek harmoniziranih standardov v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta[29].	(32) Standardizacija varnostnih zahtev je ***prostovoljen*** tržno usmerjen proces***, ki bi moral tržnim udeležencem omogočiti uporabo alternativnih sredstev za dosego vsaj podobnih rezultatov***. Da se zagotovi usklajena uporaba varnostnih standardov, bi morale države članice spodbujati uporabo in upoštevanje določenih ***interoperabilnih*** standardov ter tako zagotoviti visoko raven varnosti na ravni Unije. Zato ***je treba razmisliti o uporabi odprtih mednarodnih standardov za varnost mrežnih informacij ali o oblikovanju takih orodij***. ***Druga možnost bi bila ta, da se pripravi*** osnutek harmoniziranih standardov v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta[29]. ***Zlasti bi bilo treba ETSI, CEN in CENELEC pooblastiti za predlaganje uspešnih in učinkovitih odprtih varnostnih standardov EU, pri čemer bi se morali čim bolj izogibati dajanju prednosti določenim tehnologijam, ti standardi pa bi morali biti enostavni za uporabo s strani malih in srednjih tržnih udeležencev. Mednarodne standarde na področju kibernetske varnosti bi bilo treba temeljito preveriti, da bi zagotovili, da niso kompromisna rešitev in da nudijo ustrezno raven varnosti, kar bo tudi zagotovilo, da bo predpisana skladnost s standardi na področju kibernetske varnosti povišala splošno raven kibernetske varnosti v Uniji in ne nasprotno.***

[29] UL L 316, 14.11.2012, str. 12.

[29] UL L 316, 14.11.2012, str. 12.

Predlog spremembe 31

Predlog direktive
Uvodna izjava 33

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(33) Komisija bi morala redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim tehnološkim in tržnim razmeram.	(33) Komisija bi morala ***v posvetovanju z vsemi zainteresiranimi stranmi*** redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim ***družbenim, političnim,*** tehnološkim ali tržnim razmeram.

Predlog spremembe 32

Predlog direktive
Uvodna izjava 34

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(34) Da bi mreža za sodelovanje dobro delovala, bi bilo treba v skladu s členom 290 PDEU na Komisijo prenesti pooblastilo za sprejemanje aktov, v katerih bi ta opredelila merila, ki jih morajo države članice izpolnjevati, da lahko sodelujejo v sistemu za varno izmenjavo informacij, ter določila nadaljnje specifikacije dogodkov, ki sprožijo zgodnje opozarjanje, in opredelila okoliščine, v katerih morajo tržni udeleženci in javne uprave priglasiti incidente.	***črtano***

Predlog spremembe 33

Predlog direktive
Uvodna izjava 35

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(35) Zlasti je pomembno, da Komisija pri svojem pripravljalnem delu opravi ustrezna posvetovanja, med drugim tudi na strokovni ravni. Komisija bi morala pri pripravi in oblikovanju delegiranih aktov zagotoviti, da ustrezne dokumente istočasno, pravočasno in ustrezno predloži Evropskemu parlamentu in Svetu.	(35) Zlasti je pomembno, da Komisija pri svojem pripravljalnem delu opravi ustrezna posvetovanja, med drugim tudi ***z vsemi zainteresiranimi stranmi in predvsem*** na strokovni ravni. Komisija bi morala zagotoviti, da ustrezne dokumente istočasno, pravočasno in ustrezno predloži Evropskemu parlamentu in Svetu.

Predlog spremembe 34

Predlog direktive
Uvodna izjava 36

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(36) Da se zagotovijo enotni pogoji za izvajanje te direktive, bi bilo treba Komisiji podeliti izvedbena pooblastila v zvezi s sodelovanjem ***pristojnih organov*** in Komisije v mreži za sodelovanje, ***dostopom do infrastrukture*** za varno izmenjavo informacij, načrtom za sodelovanje Unije na področju VOI**,** oblikami in postopki, ki se uporabljajo za ***obveščanje javnosti o incidentih, ter standardi in/ali tehničnimi specifikacijami, ki se nanašajo na VOI***. Ta pooblastila bi morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije[30].	(36) Da se zagotovijo enotni pogoji za izvajanje te direktive, bi bilo treba Komisiji podeliti izvedbena pooblastila v zvezi s sodelovanjem ***enotnih kontaktnih točk*** in Komisije v mreži za sodelovanje, ***brez poseganja v obstoječe mehanizme sodelovanja na nacionalni ravni, skupnim naborom standardov*** za ***medsebojno povezovanje in varnostnih standardov za infrastrukturo za*** varno izmenjavo informacij, načrtom za sodelovanje Unije na področju VOI ***ter*** oblikami in postopki, ki se uporabljajo za ***priglasitev pomembnih incidentov***. Ta pooblastila bi morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije[30].
[30] UL L 55, 28.2.2011, str.13.	[30] UL L 55, 28.2.2011, str.13.

Predlog spremembe 35

Predlog direktive
Uvodna izjava 37

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(37) Pri izvajanju te direktive bi se Komisija morala po potrebi povezati z ustreznimi sektorskimi odbori in organi na ravni EU, zlasti na področju električne energije, prometa in zdravja.	(37) Pri izvajanju te direktive bi se Komisija morala po potrebi povezati z ustreznimi sektorskimi odbori in organi na ravni EU, zlasti na področju ***e-uprave,*** električne energije, prometa in zdravja.

Predlog spremembe 36

Predlog direktive
Uvodna izjava 38

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(38) Informacije, ki jih pristojni organ šteje za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, bi bilo treba izmenjati s Komisijo in drugimi pristojnimi organi le, če je taka izmenjava nujno potrebna za izvajanje te direktive. Izmenjane informacije bi morale biti omejene na obseg, ki ustreza namenu take izmenjave in je sorazmeren z njo.	(38) Informacije, ki jih pristojni organ ali enotna kontaktna točka šteje za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, bi bilo treba izmenjati s Komisijo***, njenimi agencijami, ki jih to zadeva, enotnimi kontaktnimi točkami in/ali*** drugimi ***nacionalnimi*** pristojnimi organi le, če je taka izmenjava nujno potrebna za izvajanje te direktive. Izmenjane informacije bi morale biti omejene na obseg, ki ustreza namenu take izmenjave in je ***potreben in*** sorazmeren z njo, ***pri tem pa bi bilo treba upoštevati vnaprej določena merila glede zaupnosti in varnosti ter protokole za določitev stopenj tajnosti, ki urejajo postopek izmenjave informacij***.

Predlog spremembe 37

Predlog direktive
Uvodna izjava 39

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom je morda potrebna obdelava osebnih podatkov. Taka obdelava osebnih podatkov je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in je zato upravičena na podlagi člena 7 Direktive 95/46/ES. V povezavi s temi upravičenimi cilji ne predstavlja nesorazmernega in nedopustnega posega, ki bi ogrožal bistvo pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije[31]. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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**.**	(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom ***ali enotnim kontaktnim točkam*** je morda potrebna obdelava osebnih podatkov. Taka obdelava osebnih podatkov je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in je zato upravičena na podlagi člena 7 Direktive 95/46/ES. V povezavi s temi upravičenimi cilji ne predstavlja nesorazmernega in nedopustnega posega, ki bi ogrožal bistvo pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije[31]. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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**.**
[31] UL L 145, 31.5.2001, str. 43.	[31] UL L 145, 31.5.2001, str. 43.

Predlog spremembe 38

Predlog direktive
Uvodna izjava 41 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(41a) Države članice so se v skladu s

	skupno politično deklaracijo držav članic in Komisije o obrazložitvenih dokumentih z dne 28. septembra 2011 zavezale, da bodo v utemeljenih primerih uradnemu obvestilu o ukrepih za prenos priložile enega ali več dokumentov, s katerimi bodo pojasnile razmerje med sestavnimi deli direktive in ustreznimi deli nacionalnih instrumentov za prenos. Zakonodajalec meni, da je predložitev takšnih dokumentov pri tej direktivi upravičena.

Predlog spremembe 39

Predlog direktive
Člen 1 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno in učinkovito obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme;	(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno in učinkovito obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme, ***ob udeležbi ustreznih zainteresiranih strani***;

Predlog spremembe 40

Predlog direktive
Člen 1 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Za izmenjavo informacij v mreži za sodelovanje v skladu s poglavjem III in za priglasitev incidentov VOI v skladu s členom 14 je morda potrebna obdelava osebnih podatkov. Taka obdelava je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in jo države članice odobrijo v skladu s členom 7 Direktive 95/46/ES in Direktivo	6. Za izmenjavo informacij v mreži za sodelovanje v skladu s poglavjem III in za priglasitev incidentov VOI v skladu s členom 14 bo morda potrebna ***komunikacija z zanesljivimi tretjimi osebami in*** obdelava osebnih podatkov. Taka obdelava je potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, in jo države članice

2002/58/ES, kakor se izvajata v nacionalni zakonodaji.	odobrijo v skladu s členom 7 Direktive 95/46/ES in Direktivo 2002/58/ES, kakor se izvajata v nacionalni zakonodaji. ***Države članice sprejmejo predpise v skladu s členom 13 Direktive 95/46/ES, da bi zagotovile, da javne uprave, tržni udeleženci in pristojni organi niso odgovorni za obdelavo osebnih podatkov, ki je potrebna za izmenjavo informacij v okviru mreže za sodelovanje in za priglasitev incidentov.***

Predlog spremembe 41

Predlog direktive
Člen 2 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Ne glede na obveznosti po zakonodaji Unije se državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo stopnjo varnosti.	Ne glede na obveznosti po zakonodaji Unije se državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo stopnjo varnosti ***in so v skladu z Listino Evropske unije o temeljnih pravicah***.

Obrazložitev

Manevrski prostor držav članic na področju varnosti je pogojen z upoštevanjem načel iz Listine Evropske unije o temeljnih pravicah, vključno z npr. pravico do spoštovanja zasebnega življenja in komunikacij, varstva osebnih podatkov, svobode gospodarske pobude in učinkovitega pravnega sredstva pred sodiščem.

Predlog spremembe 42

Predlog direktive
Člen 3 – odstavek 1 – točka 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo ***računalniških***	(b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo ***digitalnih*** podatkov

podatkov ter	ter

Predlog spremembe 43

Predlog direktive
Člen 3 – odstavek 1 – točka 1 – točka (c)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) ***računalniške*** podatke, ki jih elementi iz točke (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;	(c) ***digitalne*** podatke, ki jih elementi iz točke (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

Predlog spremembe 44

Predlog direktive
Člen 3 – odstavek 1 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da na dani ravni zaupanja prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne preko navedenih omrežij in informacijskih sistemov,	(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da na dani ravni zaupanja prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne preko navedenih omrežij in informacijskih sistemov, ***„varnost“, kot je opredeljena tukaj, zajema ustrezne tehnične naprave, rešitve in operativne postopke, ki zagotavljajo izpolnjevanje varnostnih zahtev iz te direktive;***

Predlog spremembe 45

Predlog direktive
Člen 3 – odstavek 1 – točka 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) „incident“ pomeni vsako okoliščino ali dogodek, ki ima dejanski negativen učinek na varnost;	(4) „incident“ pomeni vsako ***razumno opredeljivo*** okoliščino ali dogodek, ki ima dejanski negativen učinek na varnost;

Obrazložitev

Prvotno besedilo je bilo preširoko in bi zapletlo uporabo opredelitve.

Predlog spremembe 46

Predlog direktive
Člen 3 – odstavek 1 – točka 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(5) „storitev informacijske družbe“ pomeni storitev po točki (2) člena 1 Direktive 98/34/ES;	***črtano***

Predlog spremembe 47

Predlog direktive
Člen 3 – odstavek 1 – točka 8 – točka (a)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ponudnika storitev informacijske družbe, ki omogočajo zagotavljanje drugih storitev informacijske družbe;Priloga II vsebuje neizčrpen seznam takih ponudnikov;	***črtano***

Predlog spremembe 48

Predlog direktive
Člen 3 – odstavek 1 – točka 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo analizo, ublažitev in odzivanje na incidente;	(7) „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo ***odkrivanje, preprečevanje,*** analizo in ublažitev incidentov ter odzivanje nanje;

Predlog spremembe 49

Predlog direktive
Člen 3 – odstavek 1 – točka 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ponudnika storitev informacijske družbe, ki omogočajo zagotavljanje drugih storitev informacijske družbe;Priloga II vsebuje neizčrpen seznam takih ponudnikov;	
(b) upravljavca ***kritične*** infrastrukture, ki je bistvena za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energetike, prometa, bančništva, ***borze*** in zdravja; Priloga II vsebuje ***neizčrpen*** seznam takih upravljavcev;	(b) ***javnega ali zasebnega*** upravljavca infrastrukture, ki je bistvena za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energetike, prometa, bančništva, ***finančnih trgov*** in zdravja ***ter katere okvara ali uničenje bi pomembno negativno vplivala na državo članico zaradi nevzdrževanja teh funkcij***; Priloga II vsebuje seznam takih upravljavcev.

Predlog spremembe 50

Predlog direktive
Člen 3 – odstavek 1 – točka 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(8a) „incident z znatnim vplivom“ pomeni incident, ki vpliva na varnost in neprekinjenost informacijskega omrežja ali sistema ter povzroča velike motnje v ključnih gospodarskih in družbenih

funkcijah;

Predlog spremembe 51

Predlog direktive
Člen 3 – odstavek 1 – točka 8 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(8b) „storitev“ pomeni storitev, ki jo zagotavlja tržni udeleženec in ki ne zajema drugih storitev istega subjekta;

Predlog spremembe 52

Predlog direktive
Člen 3 – odstavek 1 – točka 11 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11a) „organizirani trg“ pomeni regulirani trg, kakor je opredeljen v točki 14 člena 4 Direktive 2004/39/ES Evropskega parlamenta in Sveta[28a];
	[28a] Direktiva 2004/39/ES Evropskega parlamenta in Sveta z dne 21. aprila 2004 o trgih finančnih instrumentov (UL L 45, 16.2.2005, str. 18).

Predlog spremembe 53

Predlog direktive
Člen 3 – odstavek 1 – točka 11 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11b) „večstranski sistem trgovanja (MTF)“ pomeni večstranski sistem trgovanja, kakor je opredeljen v točki 15

člena 4 Direktive 2004/39/ES;

Predlog spremembe 54

Predlog direktive
Člen 3 – odstavek 1 – točka 11 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11c) „sistem organiziranega trgovanja“ pomeni večstranski sistem ali instrument, ki ni organizirani trg, večstranski sistem trgovanja ali centralna nasprotna stranka, ki ga upravlja investicijsko podjetje ali tržni udeleženec ter v katerem lahko medsebojno vpliva več nakupnih in prodajnih interesov tretjih oseb v zvezi z obveznicami, strukturiranimi finančnimi produkti, emisijskimi kuponi ali izvedenimi finančnimi instrumenti, pri čemer se sklene pogodba v skladu z določbami naslova II Direktive 2004/39/ES;

Predlog spremembe 55

Predlog direktive
Člen 4 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Države članice v skladu s to direktivo zagotavljajo visoko raven varnosti omrežij in informacijskih sistemov na svojem ozemlju.	Države članice v skladu ***z Listino Evropske unije o temeljnih pravicah in*** to direktivo ***redno*** zagotavljajo visoko raven varnosti omrežij in informacijskih sistemov na svojem ozemlju.

Obrazložitev

Manevrski prostor držav članic na področju varnosti je pogojen z upoštevanjem načel iz Listine Evropske unije o temeljnih pravicah, vključno z npr. pravico do spoštovanja zasebnega življenja in komunikacij, varstva osebnih podatkov, svobode gospodarske pobude in učinkovitega pravnega sredstva pred sodiščem.

Predlog spremembe 56

Predlog direktive
Člen 5 – odstavek 1 – točka (e a) (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ea) Države članice lahko za pomoč pri oblikovanju nacionalnih strategij VOI in nacionalnih načrtov za sodelovanje na področju VOI na podlagi skupnega minimalnega načrta za strategijo in sodelovanje na področju VOI prosijo Evropsko agencijo za varnost omrežij in informacij (ENISA).

Predlog spremembe 57

Predlog direktive
Člen 5 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ***načrt ocene tveganja za prepoznavanje tveganj in ocenjevanje*** učinkov morebitnih incidentov;	(a) ***okvir za obvladovanje tveganja, vključno z opredelitvijo, razvrščanjem, oceno in obravnavo tveganj, ocenjevanjem*** učinkov morebitnih incidentov, ***možnostmi za preprečevanje in nadzor ter merili za izbiro morebitnih protiukrepov***;

Predlog spremembe 58

Predlog direktive
Člen 5 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) opredelitev vloge in odgovornosti različnih akterjev, vključenih v izvajanje ***načrta***;	(b) opredelitev vloge in odgovornosti različnih ***organov in drugih*** akterjev, vključenih v izvajanje ***okvira***;

Predlog spremembe 59

Predlog direktive
Člen 6 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Pristojni nacionalni ***organ*** za varnost omrežij in informacijskih sistemov	Pristojni nacionalni ***organi in enotne kontaktne točke*** za varnost omrežij in informacijskih sistemov

Predlog spremembe 60

Predlog direktive
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica določi ***nacionalni organ, pristojen*** za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).	1. Vsaka država članica določi ***enega ali več nacionalnih organov, pristojnih*** za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).

Predlog spremembe 61

Predlog direktive
Člen 6 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Če država članica imenuje več kot en pristojni organ, imenuje nacionalni organ, na primer pristojni organ, za enotno nacionalno kontaktno točko za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „enotna kontaktna točka“). Če država članica imenuje samo en pristojni organ, potem je ta tudi enotna kontaktna točka.

Predlog spremembe 62

Predlog direktive
Člen 6 – odstavek 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. Pristojni organi in enotna kontaktna točka iste države članice tesno sodelujejo glede obveznosti, ki jih določa ta direktiva.

Predlog spremembe 63

Predlog direktive
Člen 6 – odstavek 2 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2c. Enotna kontaktna točka zagotavlja čezmejno sodelovanje z drugimi enotnimi kontaktnimi točkami.

Predlog spremembe 64

Predlog direktive
Člen 6 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Države članice zagotovijo, da imajo pristojni organi ustrezne tehnične, finančne in človeške vire, da lahko učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnijo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje ***pristojnih organov*** prek mreže iz člena 8.	3. Države članice zagotovijo, da imajo pristojni ***organi in enotne kontaktne točke*** ustrezne tehnične, finančne in človeške vire, da lahko učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnijo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje ***enotnih kontaktnih točk*** prek mreže iz člena 8.

Predlog spremembe 65

Predlog direktive
Člen 6 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci pristojnim organom priglasijo dogodke, kot to določa člen 14(2), in da se pristojnim organom podelijo izvedbena in izvršilna pooblastila iz člena 15.	4. Države članice zagotovijo, da tržni udeleženci pristojnim organom ***in enotnim kontaktnim točkam*** priglasijo dogodke, kot to določa člen 14(2), in da se pristojnim organom podelijo izvedbena in izvršilna pooblastila iz člena 15.

Predlog spremembe 66

Predlog direktive
Člen 6 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi se po potrebi posvetujejo ***in*** sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona ***in organi za varstvo podatkov***.	5. Pristojni organi se ***redno*** posvetujejo ***z organi za varstvo podatkov***, po potrebi pa sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona.

Obrazložitev

Ravnovesje med zagotavljanjem varnosti in varovanjem svoboščin bi se podrlo, če bi nadzorna pooblastila na nacionalni ravni izvajal le en organ, brez sodelovanja z drugim dopolnilnim organom.

Predlog spremembe 67

Predlog direktive
Člen 6 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi se po potrebi posvetujejo in sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.	5. Pristojni organi ***in enotne kontaktne točke*** se po potrebi posvetujejo in sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.

Predlog spremembe 68

Predlog direktive
Člen 6 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Vsaka država članica Komisijo nemudoma obvesti o imenovanju pristojnih organov, njihovih nalogah in vseh morebitnih poznejših spremembah. Vsaka država članica javno objavi imenovanje ***pristojnega organa***.	6. Vsaka država članica Komisijo nemudoma obvesti o imenovanju pristojnih organov ***in enotne kontaktne točke***, njihovih nalogah in vseh morebitnih poznejših spremembah. Vsaka država članica javno objavi imenovanje ***pristojnih organov***.

Predlog spremembe 69

Predlog direktive
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica ustanovi skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. CERT se lahko ustanovi znotraj pristojnega organa.	1. Vsaka država članica ***za vsakega od sektorjev iz Priloge II*** ustanovi ***vsaj eno*** skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. CERT se lahko ustanovi znotraj pristojnega organa.

Predlog spremembe 70

Predlog direktive
Člen 7 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. CERT delujejo pod nadzorom pristojnega organa, ki redno pregleduje ustreznost njihovih virov, pristojnosti in učinkovitosti postopka obravnavanja	5. ***Skupine*** CERT delujejo pod nadzorom pristojnega organa ***ali enotne kontaktne točke***, ki redno pregleduje ustreznost njihovih virov, pristojnosti in učinkovitosti postopka obravnavanja incidentov.

incidentov.

Predlog spremembe 71

Predlog direktive
Člen 7 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Države članice zagotovijo, da imajo skupine CERT na voljo zadostne človeške in finančne vire za aktivno sodelovanje v mednarodnih mrežah za sodelovanje in zlasti v mrežah Unije za sodelovanje.

Predlog spremembe 72

Predlog direktive
Člen 7 – odstavek 5 – točka 1 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(1) Skupine CERT lahko dajejo pobude za skupne vaje z določenimi CERT, s CERT v vseh državah članicah in z ustreznimi institucijami držav nečlanic ter s CERT večnacionalnih in mednarodnih institucij, kot sta NATO in OZN; za tovrstne pobude in sodelovanje v skupnih vajah se te skupine tudi spodbuja.

Predlog spremembe 73

Predlog direktive
Člen 7 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Države članice lahko za pomoč pri ustanavljanju nacionalnih CERT prosijo Evropsko agencijo za varnost omrežij in

informacij (ENISA).

Predlog spremembe 74

Predlog direktive
Člen 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. ***Pristojni organi*** in Komisija vzpostavijo mrežo („mreža za sodelovanje“), v kateri sodelujejo pri preprečevanju tveganj in incidentov, ki vplivajo na omrežja in informacijske sisteme.	1. ***Enotne kontaktne točke, Evropska agencija za varnost omrežij in informacij (ENISA)*** in Komisija vzpostavijo mrežo („mreža za sodelovanje“), v kateri sodelujejo pri preprečevanju tveganj in incidentov, ki vplivajo na omrežja in informacijske sisteme.
2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in ***pristojnimi organi***. Evropska agencija za varnost omrežij in informacij (ENISA) ***na zahtevo*** mreži za sodelovanje pomaga tako, da zagotovi strokovno znanje ter svetovanje.	2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in ***enotnimi kontaktnimi točkami***. Evropska agencija za varnost omrežij in informacij (ENISA) mreži za sodelovanje pomaga tako, da zagotovi strokovno znanje ter svetovanje. ***Če je to primerno, mreža za sodelovanje sodeluje z organi za varstvo podatkov.***
3. V okviru mreže za sodelovanje ***pristojni organi***:	3. V okviru mreže za sodelovanje ***enotne kontaktne točke***:
(a) širijo zgodnja opozorila o tveganjih in incidentih v skladu s členom 10;	(a) širijo zgodnja opozorila o tveganjih in incidentih v skladu s členom 10;
(b) zagotavljajo usklajen odziv v skladu s členom 11;	(b) zagotavljajo usklajen odziv v skladu s členom 11;
(c) na skupnem spletišču redno objavljajo nezaupne informacije o tekočih zgodnjih opozorilih in usklajenem odzivu;	(c) na skupnem spletišču redno objavljajo nezaupne informacije o tekočih zgodnjih opozorilih in usklajenem odzivu;
	(ca) skupaj obravnavajo in usklajujejo ukrepe v zvezi z varnostnimi zahtevami in priglasitvijo incidentov iz člena 14 ter v zvezi z izvajanjem in izvrševanjem iz člena 15; dogovorijo se še o skupni razlagi teh ukrepov in njihovi dosledni uporabi;
(d) ***na zahtevo ene države članice ali Komisije*** v okviru področja uporabe te direktive skupaj ocenijo in razpravljajo o	(d) v okviru področja uporabe te direktive skupaj ocenijo in razpravljajo o eni ali več nacionalnih strategijah in nacionalnih

eni ali več nacionalnih strategijah in nacionalnih načrtih za sodelovanje na področju VOI iz člena 5;	načrtih za sodelovanje na področju VOI iz člena 5;
(e) na zahtevo države članice ali Komisije skupaj ocenijo in razpravljajo o učinkovitosti CERT, zlasti kadar vaje na področju VOI potekajo na ravni Unije;	(e) na zahtevo ***agencije ENISA,*** države članice ali Komisije skupaj razpravljajo o učinkovitosti CERT in jo ocenijo, zlasti kadar vaje na področju VOI potekajo na ravni Unije***, ter kar najhitreje začnejo izvajati ukrepe za odpravo ugotovljenih slabosti***;
(f) sodelujejo z ***Europolovim centrom za kibernetsko kriminaliteto in*** drugimi ustreznimi evropskimi organi ter si z njimi izmenjujejo informacije o vseh pomembnih zadevah, zlasti na področju ***varstva podatkov***, energije, prometa, bančništva, ***borze*** in zdravja;	(f) sodelujejo z drugimi ustreznimi evropskimi organi ter si z njimi izmenjujejo informacije o vseh pomembnih zadevah ***glede varnosti omrežij in informacij***, zlasti na področju energije, prometa, bančništva, ***finančnih trgov*** in zdravja;
	(fa) skupaj obravnavajo vprašanja skupne razlage, skladne uporabe in doslednega izvajanja določb iz Poglavja IV v Uniji ter se dogovarjajo o njih;
(g) med seboj in s Komisijo izmenjujejo informacije in najboljše prakse ter si pomagajo pri gradnji zmogljivosti na področju VOI;	(g) med seboj in s Komisijo izmenjujejo informacije in najboljše prakse ter si pomagajo pri gradnji zmogljivosti na področju VOI;
(h) organizirajo redne medsebojne preglede o zmogljivostih in pripravljenosti;	(h) organizirajo redne medsebojne preglede o zmogljivostih in pripravljenosti;
(i) organizirajo vaje na področju VOI na ravni Unije in po potrebi sodelujejo v mednarodnih vajah na področju VOI.	(i) organizirajo vaje na področju VOI na ravni Unije in po potrebi sodelujejo v mednarodnih vajah na področju VOI.
	(ia) dejavno spodbujajo vključevanje tržnih udeležencev ter posvetovanje in izmenjavo informacij z njimi.
	Komisija mrežo za sodelovanje redno obvešča o raziskavah na področju varnosti in drugih ustreznih programih ustreznih programih v okviru programa Obzorje 2020.
	3a. Po potrebi so lahko k sodelovanju pri dejavnostih mreže za sodelovanje, navedenih v točkah (c), (g), (h) in (i) odstavka 3, povabljeni tudi ustrezni javni organi in tržni udeleženci.

3b. Kadar se informacije, zgodnja opozorila ali najboljše prakse tržnih udeležencev ali javnih uprav izmenjujejo znotraj mreže za sodelovanje ali pa jih ta mreža razkrije, se taka izmenjava ali razkritje opravi glede na stopnjo tajnosti informacij, ki jo določi prvotni vir v skladu s členom 9(1).

3c. Komisija vsako leto objavi poročilo, ki temelji na dejavnostih mreže in na zbirnem poročilu, predloženem v skladu s členom 14(4) te direktive za preteklih 12 mesecev. Pri javnem obveščanju o posameznih incidentih, o katerih se poroča pristojnim organom in enotnim kontaktnim točkam, bi bilo treba ustrezno upoštevati ravnovesje med interesom javnosti, da je obveščena o tovrstnih grožnjah, in morebitno izgubo ugleda in gospodarsko škodo za tržne udeležence, ki so poročali o incidentih, pri čemer se javnost obvesti le po predhodnem posvetovanju.

4. Komisija z izvedbenimi akti določi potrebne načine za lažje sodelovanje med ***pristojnimi organi*** in Komisijo iz odstavkov 2 in 3. Te izvedbene akte sprejme v skladu s postopkom posvetovanja iz člena 19(2).

4. Komisija z izvedbenimi akti določi potrebne načine za lažje sodelovanje med ***enotnimi kontaktnimi točkami, agencijo ENISA*** in Komisijo iz odstavkov 2 in 3. Te izvedbene akte sprejme v skladu s postopkom posvetovanja iz člena 19(2).

Predlog spremembe 75

Predlog direktive
Člen 9 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Izmenjava občutljivih in zaupnih informacij v okviru mreže za sodelovanje se opravi prek varne infrastrukture.	Izmenjava občutljivih in zaupnih informacij v okviru mreže za sodelovanje se opravi prek varne infrastrukture, ***ki se upravlja pod nadzorom agencije ENISA***. ***Države članice zagotovijo, da se občutljive ali zaupne informacije, ki jih posredujejo druge države ali Komisija, ne bodo izmenjevale s tretjimi državami ali za***

	neustrezne namene, na primer za tajne operacije ali sprejemanje finančnih odločitev.

Predlog spremembe 76

Predlog direktive
Člen 9 – odstavek 2 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Komisija se v skladu s členom ***18*** pooblasti za sprejemanje ***delegiranih*** aktov v zvezi z opredelitvijo meril, ki morajo biti izpolnjena, da ***država članica*** lahko sodeluje v sistemu za varno izmenjavo informacij, in sicer o:	2. Komisija se v skladu s členom ***19*** pooblasti za sprejemanje ***izvedbenih*** aktov v zvezi z opredelitvijo meril, ki morajo biti izpolnjena, da lahko ***enotna kontaktna točka*** sodeluje v sistemu za varno izmenjavo informacij, in sicer o:

Predlog spremembe 77

Predlog direktive
Člen 9 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Komisija ***v skladu z merili iz odstavkov 2 in 3*** z izvedbenimi akti sprejme ***sklepe o dostopu države članice do te varne infrastrukture***. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).	3. Komisija z izvedbenimi akti sprejme ***skupen niz medsebojnih povezav in varnostnih standardov, ki jih morajo skupne kontaktne točke izpolniti za izmenjavo informacij***. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).

Predlog spremembe 78

Predlog direktive
Člen 10

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. ***Pristojni organi*** ali Komisija v mreži za sodelovanje izdajo zgodnja opozorila pri	1. ***Enotne kontaktne točke*** ali Komisija v mreži za sodelovanje izdajo zgodnja

tveganjih in incidentih, ki izpolnjujejo vsaj enega od naslednjih pogojev:	opozorila pri tveganjih in incidentih, ki izpolnjujejo vsaj enega od naslednjih pogojev:
(a) njihov obseg se hitro povečuje ali se lahko hitro poveča	
(b) ***presegajo ali lahko presežejo*** nacionalne zmogljivosti za odzivanje;	(b) ***enotna kontaktna točka oceni, da tveganje ali incident hitro narašča ali bi lahko njegov obseg hitro narastel in mogoče presegel*** nacionalne zmogljivosti za odzivanje;
(c) ***vplivajo ali lahko vplivajo*** na več kot eno državo članico.	(c) ***enotna kontaktna točka ali Komisija ocenita, da tveganje ali incident*** vpliva na več kot eno državo članico.
2. V zgodnjih opozorilih ***pristojni organi*** in Komisija sporočijo vse razpoložljive pomembne informacije, ki bi bile lahko koristne za ocenjevanje tveganja ali incidentov.	2. V zgodnjih opozorilih ***enotne kontaktne točke*** in Komisija ***brez nepotrebnega odlašanja*** sporočijo vse razpoložljive pomembne informacije, ki niso zaupne in bi bile lahko koristne za ocenjevanje tveganja ali incidentov. ***Informacije, ki jih tržni udeleženec šteje za zaupne, ter njegova identiteta se sporočijo le v obsegu, ki je potreben za oceno tveganja ali incidentov.***
3. Na zahtevo države članice ali na lastno pobudo lahko Komisija od države članice zahteva, da zagotovi vse ustrezne informacije o določenem tveganju ali incidentu.	3. Na zahtevo države članice ali na lastno pobudo lahko Komisija od države članice zahteva, da zagotovi vse ustrezne informacije o določenem tveganju ali incidentu***, ki niso zaupne***.
4. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi, da je kriminalne narave, ***pristojni organi*** ali Komisija ***o tem obvestijo Europolov center*** za kibernetsko kriminaliteto.	4. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi, da je ***resne*** kriminalne narave, ***se enotne kontaktne točke*** ali Komisija ***po potrebi in brez nepotrebnega odlašanja povežejo z nacionalnimi organi za kibernetsko kriminaliteto, da bi lahko sodelovale in izmenjavale informacije z Europolovim centrom*** za kibernetsko kriminaliteto.
	4 a. Člani mreže za sodelovanje v skladu z odstavkom 1 ne objavijo nobene prejete informacije o tveganjih in incidentih, ne da bi poprej pridobili odobritev priglasitvene enotne kontaktne točke.
	4b. Kadar se za tveganje ali incident, za katerega se izda zgodnje opozorilo, sumi,

	da je resne čezmejno-tehnične narave, enotne kontaktne točke ali Komisija o tem obvestijo agencijo ENISA;
5. Komisija se v skladu s členom ***18*** pooblasti za sprejemanje ***delegiranih*** aktov v zvezi z nadaljnjo specifikacijo tveganja in incidentov, za katere se sproži zgodnje opozarjanje iz odstavka 1.	5. Komisija se v skladu s členom ***19*** pooblasti za sprejemanje ***izvedbenih*** aktov v zvezi z nadaljnjo specifikacijo tveganja in incidentov, za katere se sproži zgodnje opozarjanje iz odstavka 1***, in v zvezi s postopki za izmenjavo informacij, ki so občutljive za tržne udeležence***.

Predlog spremembe 79

Predlog direktive
Člen 11 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Po zgodnjem opozarjanju iz člena 10 ***pristojni organi*** ocenijo ustrezne informacije in se nato dogovorijo o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI iz člena 12.	1. Po zgodnjem opozarjanju iz člena 10 ***enotne kontaktne točke*** ocenijo ustrezne informacije in se nato ***brez nepotrebnega odlašanja*** dogovorijo o usklajenem odzivu v skladu z načrtom za sodelovanje Unije na področju VOI iz člena 12.

Predlog spremembe 80

Predlog direktive
Člen 12 – odstavek 2 – točka a – alinea 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– opredelitev oblike in postopkov za zbiranje in izmenjavo združljivih in primerljivih informacij o tveganjih in incidentih s strani ***pristojnih organov***,	– opredelitev oblike in postopkov za zbiranje in izmenjavo združljivih in primerljivih informacij o tveganjih in incidentih s strani ***enotnih kontaktnih točk***,

Predlog spremembe 81

Predlog direktive

Člen 12 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Načrt za sodelovanje Unije na področju VOI se sprejme najpozneje eno leto po začetku veljavnosti te direktive in se redno pregleduje.	3. Načrt za sodelovanje Unije na področju VOI se sprejme najpozneje eno leto po začetku veljavnosti te direktive in se redno pregleduje. ***Rezultati vsakega pregleda se sporočijo Evropskemu parlamentu.***

Predlog spremembe 82

Predlog direktive
Člen 12 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Komisija zagotovi finančna sredstva za razvoj načrta Unije za sodelovanje na področju VOI.

Predlog spremembe 83

Predlog direktive
Člen 13 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. ***V takih sporazumih se upošteva potreba po zagotavljanju ustreznega*** varstva osebnih podatkov v mreži za sodelovanje.	Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. ***Ti sporazumi določajo postopek spremljanja, ki ga je treba upoštevati za zagotovitev*** varstva osebnih podatkov v mreži za sodelovanje. ***Evropski parlament se obvesti o pogajanji o sporazumih, ki morajo biti pregledna. Vsak prenos osebnih podatkov prejemnikom v državah zunaj Unije se izvede v skladu s členoma 25 in 26 Direktive 95/46/ES in členom 9 Uredbe***

(ES) št. 45/2001.

Obrazložitev

Mednarodni sporazumi, sklenjeni z drugimi državami ali varnostnimi organi, morajo vsebovati metodo spremljanja, ki zagotavlja spoštovanje državljanskih pravic. Učinkovit demokratični nadzor nad sporazumi mora izvajati tudi Evropski parlament, ki mora biti ustrezno obveščen o vsebini pogajanj o sporazumih.

Predlog spremembe 84

Predlog direktive
Člen 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci sprejmejo ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju ***trenutnega*** tehnološkega ***stanja ti*** ukrepi zagotovijo raven varnosti, primerno zadevnemu tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev in zmanjšanje vpliva ***incidentov*** na ključne storitve ***omrežij in informacijskih sistemov***, s čimer se zagotovi neprekinjenost storitev, ki jih podpirajo navedena omrežja in informacijski sistemi.	1. Države članice zagotovijo, da tržni udeleženci sprejmejo ustrezne tehnične in organizacijske ukrepe za ***odkrivanje in učinkovito*** obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju tehnološkega ***razvoja se z ustreznimi*** ukrepi zagotovi raven varnosti, ki ustreza tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev ***incidentov, ki vplivajo na varnost omrežja in informacijskih sistemov,*** in ***za*** zmanjšanje ***njihovega*** vpliva na ključne storitve omrežij in informacijskih sistemov, s čimer se zagotovi neprekinjenost storitev, ki jih podpirajo navedena omrežja in informacijski sistemi.
2. Države članice zagotovijo, da ***javne uprave in*** tržni udeleženci pristojnemu organu priglasijo incidente z ***bistvenim*** vplivom na varnost ključnih storitev, ki jih zagotavljajo.	2. Države članice ***izvajajo mehanizme , s katerimi*** zagotovijo, da tržni udeleženci pristojnemu organu ***ali enotni kontaktni točki*** priglasijo incidente z vplivom na varnost ***ali neprekinjeno opravljanje*** ključnih storitev, ki jih zagotavljajo. ***Priglasitelj zaradi prilgasitve ne nosi dodatne odgovornosti. Za opredelitev resnosti vpliva incidenta se med drugim upoštevajo naslednji parametri:***

	(a) število uporabnikov, katerih ključna storitev je prizadeta;
	(b) trajanje incidenta;
	(c) geografska razširjenost na območju, ki ga je prizadel incident.
	Ta merila se podrobneje opredelijo v skladu s členom 8(3)(ca)(novo).
	2a. Subjekti, ki jih Priloga II ne opredeljuje, lahko incidente prijavljajo prostovoljno po postopku iz člena 14(2).
	2b. Prejemnik poročila o incidentu v najkrajšem možnem času obvesti subjekt, ki je o incidentu poročal, o sprejetih ukrepih, odločitvah ali priporočilih, pa tudi o vseh obveščenih tretjih straneh in o protokolih varnosti in zaupnosti, ki urejajo izmenjavo informacij.
3. Zahteve iz odstavkov 1 in 2 veljajo za vse tržne udeležence, ki zagotavljajo storitve v EU.	3. Zahteve iz odstavkov 1 in 2 veljajo za vse tržne udeležence, ki zagotavljajo storitve v EU. ***Tržni udeleženci, ki svojih storitev ne ponujajo v Evropski uniji, lahko incidente prijavijo prostovoljno.***
	3a. Države članice zagotovijo, da tržni udeleženci priglasijo incident iz odstavkov 1 in 2 pristojnemu organu ali enotni kontaktni točki v državi članici, v kateri je prizadeta ključna storitev. Če so prizadete ključne storitve v več državah članicah, enotna kontaktna točka, ki prejme priglasitev, na podlagi informacij, ki jih posreduje tržni udeleženec, opozori ustrezne druge enotne kontaktne točke. Tržni udeleženec bo v najkrajšem možnem času obveščen o tem, katere druge enotne kontaktne točke so bile obveščene o incidentu, obveščen pa bo tudi o sprejetih ukrepih, rezultatih ali drugih pomembnih informacijah o incidentu.
4. ***Pristojni organ lahko o incidentu*** obvesti javnost ***ali to zahteva od javnih uprav in tržnih udeležencev, če ugotovi, da je razkritje incidenta v javnem interesu***. ***Nacionalni pristojni organ***	4. ***Po posvetovanju s pristojnim organom in ustreznim tržnim udeležencem lahko enotna kontaktna točka*** obvesti javnost ***o posameznih incidentih, če presodi, da je to potrebno za preprečitev incidenta ali za***

enkrat na leto mreži za sodelovanje predloži kratko poročilo o prejetih priglasitvah in ukrepih, sprejetih v skladu s tem odstavkom.

obravnavo še trajajočega incidenta oziroma če je to potrebno zato, da posamezniki sami zmanjšajo tveganja, nastala zaradi incidenta, ali če je tržni udeleženec, ki je izpostavljen incidentu, brez nepotrebnega odlašanja zavrnil obravnavanje hude strukturne ranljivosti, povezane s tem incidentom. Enotna kontaktna točka svojo odločitev ustrezno utemelji. Če je to razumno mogoče pričakovati, predstavita pristojni organ ali enotna kontaktna točka tržnim udeležencem, ki so ju obvestili o incidentu, strateško analizirane informacije, ki jim bodo pomagale pri premagovanju varnostne grožnje. Enotna kontaktna točka dvakrat na leto predloži mreži za sodelovanje kratko poročilo o prejetih priglasitvah in ukrepih, sprejetih v skladu s tem odstavkom. ***Pri javnem obveščanju o posameznih incidentih, o katerih se poroča pristojnim organom in enotnim kontaktnim točkam, bi bilo treba ustrezno upoštevati ravnovesje med interesom javnosti, da je obveščena o tovrstnih grožnjah, in morebitno izgubo ugleda in gospodarsko škodo za tržne udeležence, ki so poročali o incidentih, pri čemer se javnost obvesti le po predhodnem posvetovanju.***

Če se incidenti priglasijo mreži za sodelovanje iz člena 8, drugi nacionalni pristojni organi ne objavijo prejetih informacij v zvezi s tveganji ali incidenti brez odobritve pristojnega organa priglasitelja.

5. Komisija se v skladu s členom 18 pooblasti za sprejemanje delegiranih aktov v zvezi z opredelitvijo okoliščin, v katerih morajo javne uprave in tržni udeleženci priglasiti incidente.

6. ***Ob upoštevanju delegiranih aktov, sprejetih v skladu z odstavkom 5***, ***lahko*** pristojni organi sprejmejo smernice ***in po potrebi izdajo navodila*** glede okoliščin, v

6. Pristojni organi ***ali enotne kontaktne točke*** sprejmejo smernice glede okoliščin, v katerih morajo tržni udeleženci priglasiti incidente.

katerih morajo ***javne uprave in*** tržni udeleženci priglasiti incidente.	
7. Komisija se pooblasti, da z izvedbenimi akti določi oblike in postopke, ki se uporabljajo za namene iz odstavka 2. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).	7. Komisija se pooblasti, da z izvedbenimi akti določi oblike in postopke, ki se uporabljajo za namene iz odstavka 2. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).
8. Odstavka 1 in 2 se ne uporabljata za mikropodjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij[35].	8. Odstavka 1 in 2 se ne uporabljata za mikropodjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij[35].
_____	_____
[35] UL L 124, 20.5.2003, str. 36.	[35] UL L 124, 20.5.2003, str. 36.

Predlog spremembe 85

Predlog direktive
Člen 14 – odstavek 4 – pododstavek 1 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Poleg poročanja pristojnemu organu so tržni udeleženci spodbujeni, da v finančnih poročilih prostovoljno objavijo incidente, povezane z njihovo družbo.

Obrazložitev

Kibernetski incidenti bi lahko povzročili velike finančne izgube in znatne stroške. Delničarji in vlagatelji morajo biti seznanjeni s posledicami teh incidentov. S spodbujanjem podjetij, da prostovoljno objavljajo kibernetske incidente, se lahko spodbudi tudi medsektorska razprava o verjetnosti prihodnjih incidentov in razsežnosti teh tveganj ter sprejetje ustreznih preventivnih ukrepov za zmanjšanje kršitev kibernetske varnosti.

Predlog spremembe 86

Predlog direktive
Člen 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*

1. Države članice zagotovijo, da imajo pristojni organi ***vsa*** pooblastila, potrebna za preiskavo primerov, ***v katerih javne uprave ali tržni udeleženci ne izpolnjujejo*** obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.	1. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** pooblastila, ***s katerimi lahko zagotovijo izpolnjevanje*** obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.
2. Države članice zagotovijo, da imajo pristojni organi pooblastila, da od tržnih udeležencev ***in javnih uprav*** zahtevajo, da:	2. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** pooblastila, da od tržnih udeležencev zahtevajo, da:
(a) predložijo informacije, potrebne za oceno varnosti omrežij in informacijskih sistemov, vključno z dokumentiranimi varnostnimi ukrepi;	(a) predložijo informacije, potrebne za oceno varnosti omrežij in informacijskih sistemov, vključno z dokumentiranimi varnostnimi ukrepi;
(b) ***se zanje opravi pregled*** varnosti, ki ga ***izvede*** usposobljen neodvisen organ ali nacionalni organ, ter da se rezultati pregleda ***zagotovijo*** pristojnemu organu.	(b) ***zagotovijo dokazila o dejanskem izvajanju varnostnih politik, na primer rezultate pregleda*** varnosti, ki jih ***izvedejo notranji revizorji,*** usposobljen neodvisni organ ali nacionalni organ, in ***dokazila dajo na voljo*** pristojnemu organu ***ali enotni kontaktni točki***. ***Pristojni organ ali enotna kontaktna lahko po potrebi zahteva dodatna dokazila ali – izjemoma in z ustrezno utemeljitvijo – opravi dodaten pregled.***
	Pristojni organi in enotne kontaktne točke pri posredovanju zahteve navedejo njen namen in zadostno opredelijo, katere informacije so potrebne.
3. Države članice zagotovijo, da imajo pristojni organi pooblastila za izdajanje zavezujočih navodil za tržne udeležence ***in javne uprave***.	3. Države članice zagotovijo, da imajo pristojni organi ***in enotne kontaktne točke*** pooblastila za izdajanje zavezujočih navodil za ***vse*** tržne ***udeležence iz Priloge II***.
4. Pristojni organi incidente, za katere sumijo, da so kriminalne narave, ***priglasijo*** organom kazenskega pregona.	4. Pristojni organi ***in enotna kontaktna točka obvestijo ustrezne tržne udeležence o možnosti,*** da incidente, za katere sumijo, da so kriminalne narave, prijavijo organom kazenskega pregona.
5. Pristojni organi pri obravnavanju incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov.	5. ***Brez poseganja v veljavno zakonodajo o varstvu podatkov*** pristojni organi ***in enotne kontaktne točke*** pri obravnavanju incidentov, katerih posledica je kršitev varnosti osebnih podatkov, tesno

	sodelujejo z organi za varstvo osebnih podatkov. ***Enotne kontaktne točke in organi za varstvo podatkov v sodelovanju z agencijo ENISA razvijejo mehanizme za izmenjavo informacij in enotno predlogo, ki se uporablja za priglasitve v skladu s členom 14(2) te direktive in Direktivo 95/46 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.***
	Komisija lahko z izvedbenimi akti sprejme postopke za mehanizme izmenjave informacij in format enotne predloge, pri tem pa v največji možni meri upošteva mehanizme za izmenjavo informacij in enotne predloge, ki so jih razvile enotne kontaktne točke in organi za varstvo podatkov v sodelovanju z agencijo ENISA.
6. Države članice zagotovijo, da so obveznosti, ki se ***javnim upravam in*** tržnim udeležencem naložijo s tem poglavjem, lahko predmet sodne presoje.	6. Države članice zagotovijo, da so obveznosti, ki se tržnim udeležencem naložijo s tem poglavjem, lahko predmet sodne presoje.

Predlog spremembe 87

Predlog direktive
Člen 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Za zagotovitev usklajenega izvajanja člena 14(1) države članice spodbujajo uporabo standardov in/ali specifikacij, ki se nanašajo na varnost omrežij in informacij.	1. Za zagotovitev usklajenega izvajanja člena 14(1) države članice spodbujajo uporabo ***odprtih in interoperabilnih mednarodnih*** standardov in/ali specifikacij, ki se nanašajo na varnost omrežij in informacij, ***ne da bi predpisovale uporabo specifične tehnologije***. ***Omenjeni standardi in/ali specifikacije morajo biti v skladu z zakonodajo EU.***
2. Komisija ***z izvedbenimi akti*** pripravi seznam standardov, navedenih v odstavku	2. ***Za pripavo seznama*** standardov ***in/ali specifikacij***, navedenih v odstavku 1 ***podeli***

1. Seznam objavi v Uradnem listu Evropske unije.	Komisija ***mandat ustreznemu evropskemu organu za standardizacijo, ki seznam pripravi po posvetovanju z ustreznimi zainteresiranimi stranmi***. Seznam objavi v Uradnem listu Evropske unije.

Predlog spremembe 88

Predlog direktive
Člen 17 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice določijo pravila o sankcijah, ki se uporabljajo pri kršitvah nacionalnih predpisov, sprejetih v skladu s to direktivo, in sprejmejo vse potrebne ukrepe, da zagotovijo njihovo izvajanje. Te sankcije morajo biti učinkovite, sorazmerne in odvračilne. Države članice Komisijo o navedenih določbah obvestijo najpozneje do datuma prenosa te direktive in ji nemudoma sporočijo vse naknadne spremembe, ki vplivajo nanje.	1. Države članice določijo pravila o sankcijah, ki se uporabljajo pri kršitvah ***iz malomarnosti ali namernih kršitvah*** nacionalnih predpisov, sprejetih v skladu s to direktivo, in sprejmejo vse potrebne ukrepe, da zagotovijo njihovo izvajanje. Te sankcije morajo biti učinkovite, sorazmerne in odvračilne. Države članice Komisijo o navedenih določbah obvestijo najpozneje do datuma prenosa te direktive in ji nemudoma sporočijo vse naknadne spremembe, ki vplivajo nanje.

Obrazložitev

Pojasniti je treba, da se lahko sankcije uporabljajo za kršitve le, če tržni udeleženci niso sprejeli vseh ukrepov, ki bi se od njih lahko razumno pričakovali. V nasprotnem primeru bi to lahko odvrnilo tržne udeležence od poročanja o incidentih.

Predlog spremembe 89

Predlog direktive
Člen 17 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Države članice zagotovijo, da se sankcije iz odstavka 1 tega člena uporabijo samo, če tržni udeleženec ne izpolni svojih obveznosti iz poglavja IV namerno ali iz hude malomarnosti.

Predlog spremembe 90

Predlog direktive
Člen 18

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Člen 18	***črtano***
Izvajanje pooblastila	
1. Pooblastilo za sprejemanje delegiranih aktov se prenese na Komisijo pod pogoji iz tega člena	
2. Pooblastilo za sprejemanje delegiranih aktov iz členov 9(2), 10(5) in 14(5) se prenese na Komisijo. Komisija pripravi poročilo o prenesenem pooblastilu najpozneje devet mesecev pred iztekom petletnega obdobja. Prenos pooblastila se samodejno podaljša za enako obdobje, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred iztekom posameznega obdobja.	
3. Evropski parlament ali Svet lahko pooblastilo iz členov 9(2), 10(5) in 14(5) prekliče kadar koli. Z odločitvijo o preklicu preneha veljati prenos pooblastila, naveden v temu sklepu. Sklep začne učinkovati dan po objavi v Uradnem listu Evropske unije ali na poznejši datum, ki je v njem določen. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.	
4. Takoj ko Komisija sprejme delegirani akt, o tem istočasno uradno obvesti Evropski parlament in Svet.	
5. Delegirani akt, sprejet v skladu s členi 9(2), 10(5) in 14(5), začne veljati le, če Evropski parlament in Svet ne nasprotujeta delegiranemu aktu v dveh mesecih od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu, oziroma če sta 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 91

Predlog direktive
Člen 20 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Komisija ***redno pregleduje*** delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. Prvo poročilo predloži najpozneje ***tri leta*** po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.	Komisija ***vsaka tri leta pregleda*** delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. Prvo poročilo predloži najpozneje ***dve leti*** po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.

Obrazložitev

Da bi upoštevali spreminjajoče se nevarnosti in razmere na področju kibernetske varnosti, je treba Prilogo II redno pregledovati in urejati.

Predlog spremembe 92

Predlog direktive
Priloga 1 – naslov 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Zahteve in naloge ***skupine*** za odzivanje na računalniške grožnje (CERT)	Zahteve in naloge ***skupin*** za odzivanje na računalniške grožnje (CERT)

Predlog spremembe 93

Predlog direktive
Priloga 1 – odstavek 1 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Zahteve in naloge CERT so ustrezno in jasno opredeljene ter podprte z nacionalno politiko in/ali zakonodajo. Vključujejo naslednje elemente:	Zahteve in naloge ***skupin*** CERT so ustrezno in jasno opredeljene ter podprte z nacionalno politiko in/ali zakonodajo. Vključujejo naslednje elemente: *(Predlog spremembe velja za celotno besedilo Priloge I).*

Predlog spremembe 94

Predlog direktive
Priloga 1 – odstavek 1 – točka 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) CERT zagotavljajo visoko razpoložljivost svojih komunikacijskih storitev tako, da preprečujejo posamezne točke okvar in vzpostavijo več kanalov, po katerih se drugi lahko obračajo nanje in one obrnejo na druge. Poleg tega se komunikacijski kanali jasno opredelijo ter jih uporabniki in partnerji dobro poznajo.	(a) ***Skupine*** CERT zagotavljajo visoko razpoložljivost svojih komunikacijskih storitev tako, da preprečujejo posamezne točke okvar in vzpostavijo več kanalov, po katerih se drugi lahko ***kadar koli*** obračajo nanje in one obrnejo na druge. Poleg tega se komunikacijski kanali jasno opredelijo ter jih uporabniki in partnerji dobro poznajo.

Predlog spremembe 95

Predlog direktive
Priloga 1 – odstavek 1 – točka 1 – točka (c)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) Uradi CERT in podporni informacijski sistemi se nahajajo na varnih krajih.	(c) Uradi ***skupin*** CERT in podporni informacijski sistemi se nahajajo na varnih krajih ***z zavarovanimi omrežnimi informacijskimi sistemi***.

Predlog spremembe 96

Predlog direktive
Priloga I – odstavek 1 – točka 2 – točka a – alinea 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– spremljanje incidentov na nacionalni ravni,	– ***odkrivanje in*** spremljanje incidentov na nacionalni ravni,

Predlog spremembe 97

Predlog direktive
Priloga I – odstavek 1 – točka 2 – točka a – alinea 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	– aktivno sodelovanje v evropskih in mednarodnih mrežah za sodelovanje CERT.

Predlog spremembe 98

Predlog direktive
Priloga II

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Seznam tržnih udeležencev	Seznam tržnih udeležencev
1. Energija	1. Energija
	(a) Elektrika
	– Dobavitelji
	– Upravljavci sistemov distribucije in dobavitelji za končne uporabnike
	– Upravljavci sistema za prenos električne energije
	– Udeleženci na trgu električne energije
	(b) Nafta
	– Upravljavci cevovodov za prenos nafte in skladiščenja nafte

	– Upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in prenosa nafte
	(c) Plin
	– Dobavitelji
	– Upravljavci sistemov distribucije in dobavitelji za končne uporabnike
	– Upravljavci sistemov za prenos zemeljskega plina, upravljavci sistemov za skladiščenje in upravljavci sistemov za UZP
	– Upravljavci obratov za proizvodnjo, rafiniranje, predelavo in skladiščenje zemeljskega plina ter upravljavci prenosa zemeljskega plina
	– Udeleženci na trgu plina
2. Promet	2. Promet
	(a) Cestni promet
	(i) Izvajalci nadzora upravljanja prometa
	(ii) Pomožne logistične storitve:
	– skladiščenje in shranjevanje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti.
	(b) Železniški promet
	(i) Železnice (upravitelji infrastrukture, integrirana podjetja in prevozniki v železniškem prometu)
	(ii) Izvajalci nadzora upravljanja prometa
	(iii) Pomožne logistične storitve:
	– skladiščenje in shranjevanje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti
	(c) Letalski promet
	(i) Letalski prevozniki (tovorni in potniški zračni promet)
	(ii) Letališča
	(iii) Izvajalci nadzora upravljanja

	prometa
	(iv) Pomožne logistične storitve:
	– skladiščenje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti
	(d) Pomorski promet
	(i) Pomorski prevozniki (podjetja za notranji, pomorski in priobalni potniški in tovorni promet)
	(ii) Pristanišča
	(iii) Izvajalci nadzora upravljanja prometa
	(iv) Pomožne logistične storitve:
	– skladiščenje in shranjevanje,
	– pretovarjanje in
	– druge spremljajoče prevozne dejavnosti.
	2a. Storitve vodnega sektorja
3. Bančništvo: kreditne institucije v skladu s členom 4.1 Direktive 2006/48/ES.	3. Bančništvo: kreditne institucije v skladu s členom 4.1 Direktive 2006/48/ES.
4. Infrastruktura finančnega trga: ***borze*** in klirinške hiše centralnih nasprotnih strank	4. Infrastruktura finančnega trga: ***organizirani trgi, večstranski sistemi trgovanja, organizirani trgovalni sistemi, portali za spletna plačila*** in klirinške hiše centralnih nasprotnih strank.
5. Zdravstveni sektor: zdravstvenovarstvene ustanove (vključno z bolnišnicami in zasebnimi klinikami) ter drugi subjekti, ki zagotavljajo zdravstveno varstvo	5. Zdravstveni sektor: zdravstvenovarstvene ustanove (vključno z bolnišnicami in zasebnimi klinikami) ter drugi subjekti, ki zagotavljajo zdravstveno varstvo
	6. IKT: Računalniške storitve v oblaku, ki jih pri opravljanju storitev iz točk 1–5 uporablja upravljavec.
	Seznam se pregleda vsaki dve leti.

POSTOPEK

Naslov	Visoka skupna raven varnosti omrežij in informacij v Uniji
Referenčni dokumenti	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Pristojni odbor Datum razglasitve na zasedanju	IMCO 15.4.2013
Mnenje pripravil Datum razglasitve na zasedanju	ITRE 15.4.2013
Pridruženi odbori - datum razglasitve na zasedanju	12.9.2013
Pripravljavec/-ka mnenja Datum imenovanja	Pilar del Castillo Vera 23.5.2013
Obravnava v odboru	14.10.2013 4.11.2013
Datum sprejetja	16.12.2013
Izid končnega glasovanja	+: 36 –: 5 0: 0
Poslanci, navzoči pri končnem glasovanju	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Uručev (Vladimir Urutchev)
Namestniki, navzoči pri končnem glasovanju	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Namestniki (člen 187(2)), navzoči pri končnem glasovanju	María Auxiliadora Correa Zamora

15.1.2014

MNENJE ODBORA ZA DRŽAVLJANSKE SVOBOŠČINE, PRAVOSODJE IN NOTRANJE ZADEVE(*)

za Odbor za notranji trg in varstvo potrošnikov

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Pripravljavec mnenja: Carl Schlyter

(*) Pridruženi odbor – člen 50 Poslovnika

KRATKA OBRAZLOŽITEV

Namen predloga je doseči visoko skupno stopnjo varnosti omrežij in informacij v EU. Pripravljavec mnenja podpira cilje predloga ter priporoča spremembe, s katerimi bi izboljšali pravno varnost in okrepili zaščitne ukrepe ter varnost posameznikov in njihove zasebnosti ter s tem zagotovili, da bodo imeli posamezniki nadzor nad svojimi osebnimi podatki in bodo zaupali digitalnemu okolju, pa tudi, da bi razvili kulturo obvladovanja tveganja in izboljšali izmenjavo informacij med javnimi in zasebnimi stranmi.
Predlagane spremembe zadevajo okrepitev sklicevanja na zakonodajo o varstvu podatkov ter pojasnjujejo, da kritična infrastruktura ne bi smela vključevati družabnih omrežij in prodajaln z aplikacijami (glej spremenjeni seznam v Prilogi II), s poudarjanjem civilnega vidika podjetja pa zagotavljajo spoštovanje načela sorazmernosti: večine prekinitev in običajnih vzrokov za izpad sistema ni mogoče pripisati namernim kibernetskim napadom teroristov, kriminalcev ali tujih vohunov, temveč nenamernim človeškim napakam in naravnim vzrokom. Za EU je ključnega pomena, da izvajanje predlagane zakonodaje razloči od morebitne militarizacije te teme ter izključi cilje industrije varnosti in varovanja, ob upoštevanju okolja globaliziranega digitalnega trga.
Pomemben pomislek, ki ostaja, zadeva povezavo med predlaganim sistemom in sistemom za obveščanje, predlaganim v skladu s splošno uredbo o varstvu podatkov, ter njuno učinkovito sobivanje. Zato je treba poudariti, da bi moralo sprejetje morebitne zakonodaje EU o kibernetski varnosti slediti sprejetju splošne uredbe o varstvu podatkov, ne pa ga prehitevati. Poleg tega bi bilo treba upoštevati dejanske finančne in upravne posledice, vključno s skupnimi družbenimi stroški, ne le stroškov priglasitev. Izdelovalci programske opreme, ki so malomarni pri programiranju in varčujejo z denarjem na račun izpostavljanja svojih strank, ne morejo biti v vseh primerih zaščiteni s klavzulo v pogojih za uporabnike, s katero se zanika vsakršna odgovornost za slabo delovanje njihove programske opreme. Potrebujejo spodbude,

da zagotovijo njihovo razumno varnost. Nenazadnje pa bi bilo treba pojasniti ključne pojme (na primer pomen izrazov „javna uprava“, „znatni vpliv“ ter jasna opredelitev izraza „kibernetska kriminaliteta“), ne pa njihove razlage prepustiti državam članicam.

PREDLOGI SPREMEMB

Odbor za državljanske svoboščine, pravosodje in notranje zadeve poziva Odbor za notranji trg in varstvo potrošnikov kot pristojni odbor, da v svoje poročilo vključi naslednje predloge sprememb:

Predlog spremembe 1

Predlog direktive
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti ***in*** splošno dobro ter ***zlasti za delovanje notranjega trga***.	(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti**,** splošno dobro**,** ***komunikacijo in izmenjave med posamezniki, organizacijami civilne družbe in podjetji*** ter ***varstvo in spoštovanje zasebnega življenja in osebnih podatkov***.

Predlog spremembe 2

Predlog direktive
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Daljnosežnost in pogostnost namernih ali naključnih varnostnih incidentov se povečujeta in pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo	(2) Daljnosežnost in pogostnost namernih ali naključnih varnostnih incidentov se povečujeta in pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo

gospodarstvu Unije.	gospodarstvu Unije. ***Vedno bolj se potrjuje, da so kontrolni sistemi ranljivi na kibernetske napade z različnih strani, vključno s sovražno nastrojenimi vladami, terorističnimi skupinami in drugimi zlonamernimi vsiljivci. „Pametni“ in usklajeni napadi bi lahko imeli hude posledice za stabilnost, delovanje in ekonomiko infrastrukture.***

Predlog spremembe 3

Predlog direktive
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Kot komunikacijski instrument brez meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga.	(3) Kot komunikacijski instrument brez meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga ***ter komunikacijo in izmenjave med posamezniki, organizacijami civilne družbe in podjetji***.

Predlog spremembe 4

Predlog direktive
Uvodna izjava 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Ker so najpogostejši vzroki za izpade sistema nenamerni, na primer naravni vzroki ali človeška napaka, bi morala biti infrastruktura odporna tako proti namernim kot nenamernim prekinitvam, upravljavci kritične infrastrukture pa bi

morali izdelati sisteme, ki bodo odporni in bodo delovali tudi, kadar bi drugi sistemi zunaj njihovega nadzora odpovedali.

Predlog spremembe 5

Predlog direktive
Uvodna izjava 6 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(6a) Priznati je treba negotovost, povezano z zapletenimi sistemi, ki nas podpirajo. V ta namen je potrebno boljše skupno razumevanje tega, kaj je kritično, med tistimi, ki ščitijo organizacijo, in tistimi, ki določajo njeno strateško usmeritev.

Predlog spremembe 6

Predlog direktive
Uvodna izjava 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(8) Določbe te direktive ne bi smele posegati v možnost, da vsaka država članica sprejme potrebne ukrepe za zaščito bistvenih varnostnih interesov, zaščiti javni red in javno varnost ter preiskuje, odkriva in preganja kazniva dejanja. V skladu s členom 346 PDEU države članice niso dolžne zagotoviti informacij, za katere menijo, da bi njihovo razkritje bilo v nasprotju s ključnimi varnostnimi interesi.	(8) Določbe te direktive ne bi smele posegati v možnost, da vsaka država članica sprejme potrebne ukrepe za zaščito bistvenih varnostnih interesov, zaščiti javni red in javno varnost ter preiskuje, odkriva in preganja kazniva dejanja***, pri čemer pa tega ne bi smela uporabljati kot izgovor za neizpolnjevanje splošnejših obveznosti v zvezi z varstvom zasebnosti in osebnih podatkov***. V skladu s členom 346 PDEU države članice niso dolžne zagotoviti informacij, za katere menijo, da bi njihovo razkritje bilo v nasprotju s ključnimi varnostnimi interesi.

Predlog spremembe 7

Predlog direktive
Uvodna izjava 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni, da bo mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije.	(9) Da bi vsaka država članica dosegla in ohranila skupno visoko raven varnosti omrežij in informacijskih sistemov, bi morala imeti nacionalno strategijo VOI, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba izvesti. Načrte za sodelovanje na področju VOI, ki bi izpolnjevali bistvene zahteve, je treba pripraviti na nacionalni ravni, da bo mogoče doseči takšno raven zmogljivosti za odzivanje, ki bo v primeru incidentov omogočala uspešno in učinkovito sodelovanje na nacionalni ravni in ravni Unije ***ter spoštovala in varovala zasebno življenje in osebne podatke***.

Predlog spremembe 8

Predlog direktive
Uvodna izjava 10

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(10) Da se zagotovi učinkovito izvajanje določb, sprejetih v skladu s to direktivo, bi bilo treba v vsaki državi ustanoviti ali določiti organ za usklajevanje vprašanj VOI***, ki bi*** deloval kot osrednja točka za čezmejno sodelovanje na ravni Unije. Ti organi bi morali imeti ustrezne tehnične, finančne in človeške vire, da bi lahko uspešno in učinkovito opravljali dodeljene naloge ter tako dosegli cilje te direktive.	(10) Da se zagotovi učinkovito izvajanje določb, sprejetih v skladu s to direktivo, bi bilo treba v vsaki državi ustanoviti ali določiti ***nacionalni pristojni*** organ ***pod civilnim nadzorom,*** za ***katerega bi veljala popoln demokratični nadzor in preglednost dejavnosti ter bi bil odgovoren za*** usklajevanje vprašanj VOI ***in*** deloval kot osrednja točka za čezmejno sodelovanje na ravni Unije. Ti organi bi morali imeti ustrezne tehnične, finančne in človeške vire, da bi lahko uspešno in učinkovito opravljali dodeljene naloge ter tako dosegli cilje te direktive.

Predlog spremembe 9

Predlog direktive
Uvodna izjava 14 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(14a) V vse več sektorjih se v računalniško okolje uvajajo storitve v oblaku, kot so storitve informacijske tehnologije, ki upravljajo kritično infrastrukturo. Zadostni varnostni ukrepi morajo zagotavljati zaupnost, celovitost in razpoložljivost podatkov v oblaku. Gostovanje infrastrukturnih storitev in shranjevanje občutljivih podatkov v okolju računalništva v oblaku s seboj prinaša zahteve glede varnosti in odpornosti, ki jih obstoječe storitve v oblaku ne morejo ustrezno izpolniti. Zato je potrebno zagotovilo, da lahko okolje računalništva v oblaku zagotavlja ustrezno varstvo občutljivih infrastrukturnih podatkov.

Predlog spremembe 10

Predlog direktive
Uvodna izjava 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem ***ter*** si izmenjevati informacije in najboljše prakse ***v zameno za*** operativno podporo pri incidentih.	(15) Ker večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Tržne udeležence bi bilo treba spodbujati, da za zagotavljanje VOI vzpostavijo lastne neformalne mehanizme sodelovanja. Prav tako bi morali sodelovati z javnim sektorjem***,*** si ***vzajemno*** izmenjevati informacije in najboljše prakse ***ter drug drugemu zagotavljati potrebno*** operativno podporo pri incidentih.

Predlog spremembe 11

Predlog direktive
Uvodna izjava 15 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(15a) Po možnosti in v skladu z Direktivo 95/46ES bi bilo treba v celoti upoštevati že obstoječe nacionalne mehanizme sodelovanja med javnimi in zasebnimi udeleženci, določbe iz te direktive pa teh vzpostavljenih dogovorov o sodelovanju ne bi smele ogroziti.

Predlog spremembe 12

Predlog direktive
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi morali pristojni organi vzpostaviti skupno spletišče, na katerem bi objavljali nezaupne informacije o incidentih in tveganjih.	(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi morali pristojni organi vzpostaviti skupno spletišče, na katerem bi ***nemudoma*** objavljali ***celovite*** nezaupne informacije o incidentih in tveganjih.

Predlog spremembe 13

Predlog direktive
Uvodna izjava 21

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(21) Zaradi globalne narave težav na področju VOI je potrebno tesnejše mednarodno sodelovanje, da se izboljšajo varnostni standardi in izmenjava informacij ter spodbuja skupen globalen pristop za vprašanja VOI.	(21) Zaradi globalne narave težav na področju VOI je potrebno tesnejše mednarodno sodelovanje, da se izboljšajo varnostni standardi in izmenjava informacij ter spodbuja skupen globalen pristop za vprašanja VOI***, pod pogojem, da imajo države, s katerimi je predvideno to sodelovanje, instrumente za nadzor in varstvo podatkov, ki zagotavljajo enako varnost kot instrumenti EU***.

Predlog spremembe 14

Predlog direktive
Uvodna izjava 22

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(22) Odgovornost za zagotavljanje VOI imajo v veliki meri javne uprave in ***tržni udeleženci***. Kulturo obvladovanja tveganja, ki vključuje oceno tveganja in izvajanje ***ustreznih*** varnostnih ukrepov ***za zadevna tveganja***, bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. Vzpostavitev enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.	(22) Odgovornost za zagotavljanje VOI imajo v veliki meri javne uprave in ***podjetja***. Kulturo obvladovanja tveganja, ki vključuje oceno tveganja in izvajanje varnostnih ukrepov, ***namenjenih predvidevanju namernih ali naključnih varnostnih incidentov,*** bi bilo treba spodbujati in razvijati z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami. ***Kjer taka kultura obvladovanja tveganja že obstaja, zlasti če se opira na prostovoljne prakse, bi jo bilo treba podpirati, krepiti in širiti.*** Vzpostavitev enakih konkurenčnih pogojev je prav tako bistvenega pomena za učinkovito delovanje mreže za sodelovanje, saj bi zagotovila učinkovito sodelovanje vseh držav članic.

Predlog spremembe 15

Predlog direktive
Uvodna izjava 22 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(22a) Javne uprave in zasebna podjetja, vključno s ponudniki omrežnih in informacijskih storitev ter programske opreme, bi morali zaščito svojih informacijskih sistemov in podatkov, ki jih vsebujejo, šteti za del svoje dolžne skrbnosti. Zagotoviti bi bilo treba ustrezno raven zaščite glede na razumno določljive grožnje in področja ranljivosti. Stroški in obremenitve take zaščite bi morali odražati verjetno škodo, ki bi jo kibernetski napad povzročil prizadetim osebam.

Predlog spremembe 16

Predlog direktive
Uvodna izjava 26 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(26a) Otroci so že zelo zgodaj v življenju izpostavljeni internetu in drugi sodobni tehnologiji ter nevarnostim, povezanim s tem. Ustrezno upravljanje otrokom prijaznega spletnega prostora je bistveno za zmanjševanje nevarnosti ter zagotavljanje, da zaščita otrok in varstvo njihovih pravic nista ogrožena.

Predlog spremembe 17

Predlog direktive
Uvodna izjava 28

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(28) Pristojni organi bi morali ustrezno pozornost nameniti ohranjanju neuradnih in zanesljivih kanalov za izmenjavo informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom, bi bilo treba ***najti ravnotežje med interesom*** javnosti, da je obveščena o nevarnostih, ***ter morebitno škodo za ugled in poslovanje javnih uprav in tržnih udeležencev, ki priglasijo incidente. Pri izvajanju obveznosti priglasitve bi morali pristojni organi posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne do ustreznega popravila varnosti.***	(28) Pristojni organi bi morali ustrezno pozornost nameniti ohranjanju neuradnih in zanesljivih kanalov za izmenjavo informacij med tržnimi udeleženci ter med javnim in zasebnim sektorjem. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom, bi bilo treba ***dati prednost interesu*** javnosti, da je obveščena o nevarnostih, ***pred kratkoročnimi gospodarskimi dejavniki.***

Predlog spremembe 18

Predlog direktive
Uvodna izjava 29 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(29a) Zloraba interneta omogoča organiziranemu kriminalu, da prek spleta širi svoje dejavnosti, katerih namen je pranje denarja, ponarejanje ter ponujanje drugih izdelkov in storitev, ki kršijo pravice intelektualne lastnine, ter preskušanje novih kriminalnih dejavnosti, kar kaže na njegovo zaskrbljujočo sposobnost prilagajanja sodobnim tehnologijam.

Predlog spremembe 19

Predlog direktive
Uvodna izjava 30 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(30a) Kibernetska kriminaliteta povzroča vse večjo gospodarsko in socialno škodo, ki prizadene več milijonov potrošnikov in po podatkih povzroči letne izgube v višini 290 milijard EUR[4a].
	[4a] Poročilo o kibernetski kriminaliteti družbe Norton za leto 2012 (Norton Cybercrime Report 2012).

Predlog spremembe 20

Predlog direktive
Uvodna izjava 33

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(33) Komisija bi morala redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim tehnološkim in tržnim razmeram.	(33) Komisija bi morala redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim tehnološkim in tržnim razmeram ***ter obveznostim zagotavljanja najvišje ravni varnosti in celovitosti omrežij in informacij, varstva zasebnosti in osebnih***

podatkov.

Predlog spremembe 21

Predlog direktive
Uvodna izjava 39

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom je morda potrebna obdelava osebnih podatkov. Taka obdelava osebnih podatkov ***je*** potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, ***in je zato*** upravičena na podlagi člena 7 Direktive 95/46/ES. ***V povezavi s temi upravičenimi cilji ne predstavlja nesorazmernega in nedopustnega posega***, ki ***bi ogrožal bistvo*** pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije[31]. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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.	(39) Za izmenjavo informacij o tveganjih in incidentih v mreži za sodelovanje in za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom je morda potrebna obdelava osebnih podatkov. ***Če je*** taka obdelava osebnih podatkov potrebna za doseganje ciljev javnega interesa, za katere si prizadeva ta direktiva, ***je lahko*** upravičena na podlagi člena 7 Direktive 95/46/ES. ***Vendar to pristojnih organov ne odvezuje obveznosti sorazmernega ukrepanja na način***, ki ***verjetno ne ogroža*** pravice do varstva osebnih podatkov iz člena 8 Listine o temeljnih pravicah. Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije[31]. Obdelava podatkov v institucijah in organih Unije za namene izvajanje te direktive bi morala biti skladna z Uredbo (ES) št. 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.
[31] UL L 145, 31.05.01, str. 43.	[31] UL L 145, 31.05.01, str. 43.

Predlog spremembe 22

Predlog direktive
Uvodna izjava 41 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(41a) Pri vseh ukrepih bi bilo treba zagotoviti varstvo temeljnih človekovih pravic, zlasti pravic iz Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (člen 8, zasebno življenje), in upoštevanje „načela sorazmernosti“.

Predlog spremembe 23

Predlog direktive
Člen 1 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Ta direktiva ***prav tako ne posega*** v Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ter Uredbo Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.	5. Ta direktiva v ***celoti spoštuje*** Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ter Uredbo ***(ES) št. 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.

Predlog spremembe 24

Predlog direktive
Člen 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Ne glede na obveznosti po zakonodaji Unije se državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo stopnjo varnosti.	Ne glede na obveznosti po zakonodaji Unije se državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo stopnjo varnosti***, vendar morajo take določbe ustrezati skupnim minimalnim pričakovanjem iz te direktive, ki se uporabljajo v tem primeru***.

Predlog spremembe 25

Predlog direktive
Člen 3 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da ***na dani ravni zaupanja*** prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne ***preko*** navedenih omrežij in informacijskih sistemov,	(2) „varnost“ pomeni zmožnost omrežja ali informacijskega sistema, da prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne ***prek*** navedenih omrežij in informacijskih sistemov,

Predlog spremembe 26

Predlog direktive
Člen 3 –odstavek 2 – točka a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	„kibernetska odpornost“ pomeni zmožnost omrežnega in informacijskega sistema, da vzdrži in obnovi polno operativno zmogljivost po incidentih, med drugim po tehnični motnji, izpadu energije ali varnostnemu incidentu;

Predlog spremembe 27

Predlog direktive
Člen 3 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
„incident“ pomeni vsako okoliščino ali dogodek, ki ima dejanski negativen učinek na varnost;	„incident“ pomeni vsako okoliščino ali dogodek, ki ima dejanski negativen učinek na varnost ***in na zagotavljanje ključnih storitev***;

Predlog spremembe 28

Predlog direktive
Člen 3 – točka 8 – točka (b)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) upravljavca kritične infrastrukture, ki je bistvena za vzdrževanje ključnih gospodarskih ***in družbenih*** dejavnosti na področjih energetike, prometa, bančništva, borze in zdravja; Priloga II vsebuje neizčrpen seznam takih upravljavcev;	(b) upravljavca kritične infrastrukture, ki je bistvena za vzdrževanje ključnih ***družbenih in*** gospodarskih dejavnosti na področjih energetike, prometa, bančništva, borze***, verige preskrbe s hrano*** in zdravja; Priloga II vsebuje neizčrpen seznam takih upravljavcev;

Predlog spremembe 29

Predlog direktive
Člen 5 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) ***načrt ocene tveganja*** za prepoznavanje tveganj in ocenjevanje učinkov morebitnih incidentov;	(a) ***okvir*** za ***obvladovanje tveganj, ki zajema najmanj redno oceno tveganj za*** prepoznavanje tveganj in ocenjevanje učinkov morebitnih incidentov ***ter ukrepe za ohranjanje varnosti in celovitosti informacij, vključno z zgodnjim opozarjanjem***;

Obrazložitev

Načrt ocene je nezadosten in ne vsebuje drugih potrebnih ukrepov za obvladovanje tveganj na področju varnosti omrežij in informacij. Evropski nadzornik za varstvo podatkov priporoča

vzpostavitev okvira za obvladovanje tveganj, ki vključuje oceno tveganja.

Predlog spremembe 30

Predlog direktive
Člen 5 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI se sporočita Komisiji v enem mesecu po sprejetju.	3. Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI se sporočita Komisiji***, Evropskemu parlamentu, Svetu in Evropskemu nadzorniku za varstvo podatkov*** v enem mesecu po sprejetju***, kar je najpozneje 12 mesecev od začetka veljavnosti te direktive***.

Predlog spremembe 31

Predlog direktive
Člen 5 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Komisija pripravi povzetek strategij VOI vseh držav članic in ga posreduje vsem državam članicam v organizirani obliki.

Obrazložitev

Koristno bo, če bodo imele države članice tudi vpogled v načrte drugih držav. To jim bo pomagalo pri oblikovanju njihovih pristopov in je lahko priložnost za izmenjavo primerov dobre prakse.

Predlog spremembe 32

Predlog direktive
Člen 5 – odstavek 3 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3b) Komisija v šestih mesecih po sprejetju te direktive pripravi smernice o

	strukturi strategije VOI. Namen teh smernic je pomagati državam članicam pri oblikovanju in sprejemanju dokumentov s približno enako strukturo.

Obrazložitev

Organiziranje in povzemanje na podlagi 28 dokumentov na ravni Skupnosti utegneta biti učinkovitejša, če bodo ti dokumenti imeli določeno splošno strukturo. Čeprav smernice Komisije ne bi bile zavezujoče, bi v vsakem primeru spodbudile države članice k upoštevanju tega priporočenega modela/strukture pri oblikovanju nacionalnih strategij.

Predlog spremembe 33

Predlog direktive
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica določi nacionalni organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).	1. Vsaka država članica določi ***civilni*** nacionalni organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).

Predlog spremembe 34

Predlog direktive
Člen 6 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi se po potrebi posvetujejo in sodelujejo ***z ustreznimi*** nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.	5. Pristojni organi se po potrebi posvetujejo in ***tesno*** sodelujejo ***s pristojnimi*** nacionalnimi organi kazenskega pregona in organi za varstvo podatkov ***ter upoštevajo načelo sorazmernosti***.

Predlog spremembe 35

Predlog direktive
Člen 6 – odstavek 5 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Pristojni organi pri zbranih, obdelanih

	in izmenjanih informacijah izpolnjujejo zahteve o varstvu osebnih podatkov iz člena 17 Direktive št. 95/46/ES.

Predlog spremembe 36

Predlog direktive
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica ustanovi skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. CERT se ***lahko*** ustanovi znotraj pristojnega organa.	1. Vsaka država članica ustanovi skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I. CERT se ***po potrebi*** ustanovi znotraj pristojnega organa.

Predlog spremembe 37

Predlog direktive
Člen 8 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in pristojnimi organi. Evropska agencija za varnost omrežij in informacij (ENISA) na zahtevo mreži za sodelovanje pomaga tako, da zagotovi ***strokovno znanje ter svetovanje***.	2. Z mrežo za sodelovanje se vzpostavi trajna komunikacija med Komisijo in pristojnimi organi. Evropska agencija za varnost omrežij in informacij (ENISA) na zahtevo mreži za sodelovanje pomaga tako, da zagotovi ***tehnološko nevtralne smernice s primernimi ukrepi tako za javne kot zasebne sektorje***.

Predlog spremembe 38

Predlog direktive
Člen 9 – odstavek 2 – točka (b a) (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) merilih za sodelovanje držav članic v sistemu za varno izmenjavo informacij,

	katerih namen je zagotoviti, da vse sodelujoče države na vseh stopnjah obdelave zagotavljajo visoko raven varnosti in odpornosti, tudi z ustreznimi ukrepi za zaupnost in varnost v skladu s členoma 16 in 17 Direktive št. 95/46/ES in členoma 21 in 22 Uredbe (ES) št. 45/2001.

Predlog spremembe 39

Predlog direktive
Člen 9 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Komisija v skladu z merili iz odstavkov 2 in 3 z izvedbenimi akti sprejme sklepe o dostopu države članice do te varne infrastrukture. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).	***črtano***

Predlog spremembe 40

Predlog direktive
Člen 12 – odstavek 2 – točka a – alinea 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– opredelitev ***postopkov in*** meril za oceno tveganja in incidentov v mreži za sodelovanje.	– opredelitev meril za oceno tveganja in incidentov v mreži za sodelovanje.

Predlog spremembe 41

Predlog direktive
Člen 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki	Ne glede na možnost, da se lahko v okviru mreže za sodelovanje neformalno sodeluje na mednarodni ravni, lahko Unija sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki

omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. ***V takih sporazumih se upošteva potreba po zagotavljanju ustreznega*** varstva osebnih podatkov v mreži za sodelovanje.	omogočajo njihovo sodelovanje pri nekaterih dejavnostih mreže za sodelovanje. ***Ti sporazumi se sprejmejo le, če je mogoče zagotoviti raven*** varstva osebnih podatkov v mreži za sodelovanje***, ki ustreza in je primerljiva z ravnjo v Uniji***.

Predlog spremembe 42

Predlog direktive
Člen 14 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice zagotovijo, da javne uprave in tržni udeleženci sprejmejo ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju trenutnega tehnološkega stanja ti ukrepi zagotovijo raven varnosti, primerno zadevnemu tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev in zmanjšanje vpliva incidentov na ključne storitve omrežij in informacijskih sistemov, s čimer se zagotovi neprekinjenost storitev, ki jih podpirajo navedena omrežja in informacijski sistemi.	1. Države članice zagotovijo, da javne uprave in tržni udeleženci sprejmejo ustrezne tehnične in organizacijske ukrepe za ***odkrivanje, učinkovito*** obvladovanje ***in omejevanje*** tveganj za varnost omrežij in informacijskih sistemov, ki jih nadzorujejo in uporabljajo pri svojih dejavnostih. Ob upoštevanju trenutnega tehnološkega stanja ti ukrepi zagotovijo raven varnosti, primerno ***in sorazmerno*** zadevnemu tveganju. Ti ukrepi se sprejmejo zlasti za preprečitev in zmanjšanje vpliva incidentov na ključne storitve omrežij in informacijskih sistemov, s čimer se zagotovi neprekinjenost storitev ***in varnosti podatkov***, ki jih podpirajo navedena omrežja in informacijski sistemi.

Predlog spremembe 43

Predlog direktive
Člen 14 –odstavek 2 točka a (novo)

	Predlog spremembe
	(a) Proizvajalci komercialne programske opreme so kljub določbam o neprevzemanju odgovornosti v sporazumih z uporabniki odgovorni v primeru hude malomarnosti v zvezi z

varnostjo in zaščito.

Obrazložitev

Proizvajalci komercialne programske opreme v licenčni pogodbi zavračajo kakršno koli odgovornost, ki lahko izhaja iz zagotovitve neustrezne varnosti in slabega programiranja. Da bi spodbudili proizvajalce programske opreme k vlaganju v varnostne ukrepe, je potrebna drugačna kultura. To je mogoče uresničiti le, če bodo proizvajalci programske opreme odgovorni za vse pomanjkljivosti v varnosti.

Predlog spremembe 44

Predlog direktive
Člen 14 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Zahteve iz odstavkov 1 in 2 veljajo za vse tržne udeležence, ki zagotavljajo storitve v EU.	3. Zahteve iz odstavkov 1 in 2 veljajo za vse tržne udeležence ***in proizvajalce programske opreme***, ki zagotavljajo storitve v EU.

Predlog spremembe 45

Predlog direktive
Člen 14 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. Ob upoštevanju delegiranih aktov, sprejetih v skladu z odstavkom 5, lahko pristojni organi sprejmejo smernice in po potrebi izdajo navodila glede okoliščin, v katerih morajo javne uprave in tržni udeleženci priglasiti incidente.	***črtano***

Predlog spremembe 46

Predlog direktive
Člen 15 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Države članice zagotovijo, da imajo pristojni organi ***vsa*** pooblastila, potrebna	1. Države članice zagotovijo, da imajo pristojni organi pooblastila, potrebna za

za preiskavo primerov, v katerih javne uprave ali tržni udeleženci ne izpolnjujejo obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.	preiskavo primerov, v katerih javne uprave ali tržni udeleženci ne izpolnjujejo obveznosti iz člena 14, in posledic takšnega neizpolnjevanja za varnost omrežij in informacijskih sistemov.

Predlog spremembe 47

Predlog direktive
Člen 15 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Pristojni organi pri obravnavanju incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov.	5. ***Brez poseganja v veljavno zakonodajo o varstvu podatkov in po temeljitem posvetovanju z ustreznimi upravljavci in obdelovalci podatkov*** pristojni organi ***in enotne kontaktne točke*** pri obravnavanju incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov.

Predlog spremembe 48

Predlog direktive
Člen 19 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 19a
	Varstvo in obdelava osebnih podatkov
	1. Vsaka obdelava osebnih podatkov v državah članicah na podlagi te direktive se izvaja v skladu z Direktivo 95/46/ES in Direktivo 2002/58/ES.
	2. Vsaka obdelava osebnih podatkov s strani Komisije in agencije ENISA na podlagi te uredbe se izvaja v skladu z Uredbo (ES) št. 45/2001.
	3. Vsaka obdelava osebnih podatkov s strani Europolovega centra za kibernetski kriminal za namene te direktive se izvaja v skladu s Sklepom 2009/371/PNZ.

	4. Obdelava osebnih podatkov je poštena in zakonita ter strogo omejena na najmanjšo količino podatkov, ki je potrebna za namene, za katere se ti podatki obdelujejo. Osebni podatki se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namen, za katerega se osebni podatki obdelujejo.
	5. Priglasitev incidentov iz člena 14 ne posega v določbe in obveznosti v zvezi z obveščanjem o kršitvi varnosti osebnih podatkov iz člena 4 Direktive 2002/58/ES in Uredbe (EU) št. 611/2013.
	6. Sklicevanja na Direktivo 95/46/ES se z začetkom veljavnosti uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (splošna uredba o varstvu podatkov) razlagajo kot sklicevanja na omenjeno uredbo.

Predlog spremembe 49

Predlog direktive
Člen 20 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Komisija redno pregleduje delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. Prvo poročilo predloži najpozneje ***tri leta*** po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.	Komisija redno pregleduje delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. Prvo poročilo predloži najpozneje ***dve leti*** po datumu prenosa iz člena 21. V ta namen lahko Komisija zahteva, da države članice zagotovijo informacije brez nepotrebnega odlašanja.

Predlog spremembe 50

Predlog direktive
Priloga 1 – odstavek 1 – točka 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) CERT izvajajo in upravljajo varnostne ukrepe, s čimer zagotovijo zaupnost, celovitost, razpoložljivost in verodostojnost informacij, ki jih prejmejo in obravnavajo.	(b) CERT izvajajo in upravljajo varnostne ukrepe, s čimer zagotovijo zaupnost, celovitost, razpoložljivost in verodostojnost informacij, ki jih prejmejo in obravnavajo***, ter varstvo podatkov***.

Predlog spremembe 51

Predlog direktive
Priloga 2 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Seznam tržnih udeležencev	Seznam tržnih udeležencev
Iz člena 3(8)a):	Iz člena 3(8)a):
1. Platforme za e-trgovanje	1. Platforme za e-trgovanje
2. Portali za spletna plačila	2. Portali za spletna plačila
3. Družabna omrežja	
4. Iskalniki	***3***. Iskalniki
5. Računalniške storitve v oblaku	***4***. Računalniške storitve v oblaku***, ki shranjujejo podatke o kritični infrastrukturi Evropske unije***
6. Prodajalne z aplikacijami	

Predlog spremembe 52

Predlog direktive
Priloga 2 – odstavek 2 – točka 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Veriga preskrbe s hrano

POSTOPEK

Naslov	Visoka skupna raven varnosti omrežij in informacij v Uniji
Referenčni dokumenti	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Pristojni odbor Datum razglasitve na zasedanju	IMCO 15.4.2013
Mnenje pripravil Datum razglasitve na zasedanju	LIBE 15.4.2013
Pridruženi odbori - datum razglasitve na zasedanju	12.9.2013
Pripravljavec/-ka mnenja Datum imenovanja	Carl Schlyter 7.3.2013
Obravnava v odboru	25.4.2013 18.9.2013 4.11.2013 13.1.2014
Datum sprejetja	13.1.2014
Izid končnega glasovanja	+: 36 –: 6 0: 0
Poslanci, navzoči pri končnem glasovanju	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, baronica Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra
Namestniki, navzoči pri končnem glasovanju	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria
Namestniki (člen 187(2)), navzoči pri končnem glasovanju	Katarína Neveďalová

6.12.2013

MNENJE ODBORA ZA ZUNANJE ZADEVE

za Odbor za notranji trg in varstvo potrošnikov

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Pripravljavka mnenja: Ana Gomes

PREDLOGI SPREMEMB

Odbor za zunanje zadeve poziva Odbor za notranji trg in varstvo potrošnikov kot pristojni odbor, da v svoje poročilo vključi naslednje predloge sprememb:

Predlog spremembe 1

Predlog direktive
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga.	(1) Omrežja ter informacijski sistemi in storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske dejavnosti in splošno dobro ter zlasti za delovanje notranjega trga ***in zunanjo varnost EU***.

Predlog spremembe 2

Predlog direktive
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Daljnosežnost in pogostnost namernih ali naključnih varnostnih incidentov se	(2) Daljnosežnost in pogostnost namernih ali naključnih varnostnih incidentov se

povečujeta in pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo gospodarstvu Unije.	povečujeta in pomenita veliko tveganje za delovanje omrežij in informacijskih sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, zmanjšujejo zaupanje uporabnikov in povzročijo veliko škodo gospodarstvu Unije ***ter ogrožajo dobrobit državljanov EU in sposobnost držav članic EU, da se zaščitijo in zagotovijo varnost kritične infrastrukture***.

Predlog spremembe 3

Predlog direktive
Uvodna izjava 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2a) Solidarnostna klavzula iz člena 222 PDEU predstavlja ustrezen okvir za pomoč in usklajeno delovanje držav članic EU v primeru terorističnega napada ali kriminalne dejavnosti, ki bi ogrozila varnost omrežij in informacij. Prav tako klavzula o vzajemni obrambi iz člena 42(7) PEU predstavlja okvir za delovanje znotraj EU v primeru, da bi država članica postala žrtev oboroženega napada, ki bi zmanjšal varnost omrežij in informacij. V zadevnih primerih bi bilo treba člen 222 PDEU in člen 42(7) PEU uporabljati tako, da se dopolnjujeta.

Predlog spremembe 4

Predlog direktive
Uvodna izjava 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(2a) Veliko število kibernetskih incidentov se zgodi zaradi pomanjkanja vzdržljivosti in odpornosti zasebne in javne omrežne infrastrukture, slabo zaščitenih ali varovanih zbirk podatkov in drugih

	pomanjkljivosti v kritični informacijski infrastrukturi; ker le malo držav članic obravnava zaščito svojih omrežij in informacijskih sistemov ter s tem povezanih podatkov kot del svojih dolžnosti, kar pojasnjuje pomanjkanje vlaganj v sodobno varnostno tehnologijo, usposabljanje in razvoj ustreznih smernic.

Predlog spremembe 5

Predlog direktive
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Kot komunikacijski instrument brez meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga.	(3) Kot komunikacijski instrument brez meja imajo digitalni informacijski sistemi, zlasti internet, bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in oseb. Zaradi te nadnacionalne narave lahko znatne prekinitve navedenih sistemov v eni državi članici vplivajo tudi na druge države članice in Unijo kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga ***ter za notranjo in zunanjo varnost EU. Potrebo po izboljšanju varnosti omrežij in informacij bi bilo zato treba ustrezno poudariti v strategiji notranje varnosti Unije in evropski varnostni strategiji, zlasti kar zadeva prihodnjo revizijo teh dokumentov.***

Predlog spremembe 6

Predlog direktive
Uvodna izjava 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Ozaveščanje in izobraževanje uporabnikov informacijskih in

komunikacijskih tehnologij o najboljših praksah, varstvu osebnih podatkov in trajnem vzdrževanju komunikacijskih storitev bi moral biti temelj vsake celovite strategije za kibernetsko varnost.

Predlog spremembe 7

Predlog direktive
Uvodna izjava 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4a) Sodelovanje in usklajevanje med ustreznimi evropskimi organi z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko in podpredsednikom Komisije, in koordinatorjem EU za boj proti terorizmu bi bilo treba zagotoviti v vseh primerih, ko lahko sklepamo, da gre za tveganje zunanje ali teroristične narave.

Predlog spremembe 8

Predlog direktive
Uvodna izjava 4 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4b) Izmenjavo obveščevalnih in občutljivih podatkov med državami članicami ter med državami članicami in pristojnimi organi EU bi bilo treba okrepiti in utemeljiti na načelih zaupanja, solidarnosti in sodelovanja. Zato bi moral vsak akcijski načrt za izboljšanje varnosti omrežij in sistemov v celoti uporabiti že obstoječe strukture znotraj EU, kot sta situacijski center EU in center EU za analizo obveščevalnih podatkov, ter zagotoviti usklajevanje med vsemi strukturami, ki vplivajo na varnost informacij, ki so pomembne za notranjo in zunanjo varnost EU.

Predlog spremembe 9

Predlog direktive
Uvodna izjava 4 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(4c) Glede na nadnacionalni značaj groženj sta sodelovanje in izmenjava podatkov na svetovni ravni z zadevnimi mednarodnimi partnerji bistvena za učinkovito strategijo kibernetske varnosti in premišljeno delovanje v smeri izboljšanja varnosti omrežij in informacij znotraj EU.

Predlog spremembe 10

Predlog direktive
Uvodna izjava 8 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(8a) Varnostni ukrepi morajo spoštovati temeljne pravice, h katerim so se zavezale EU in njene države članice v skladu s členi 2, 6 in 21 PDEU, kot so svoboda izražanja, varstvo podatkov in zasebnost; ker sta pravici do zasebnosti in varstva podatkov določeni v Listini EU in členu 16 PDEU;

Predlog spremembe 11

Predlog direktive
Uvodna izjava 11 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(11a) Vse države članice se morajo pri nacionalnih strategijah za kibernetsko varnost osredotočiti na zaščito

	informacijskih sistemov in z njimi povezanih podatkov ter morajo zaščito kritične infrastrukture obravnavati kot del svojih dolžnosti. Države članice morajo sprejeti in izvajati strategije, smernice in instrumente, ki zagotavljajo razumne ravni zaščite pred razumno opredeljivimi ravnmi groženj, s stroški in obremenitvami zaščite, ki so sorazmerni z verjetno škodo za zadevne strani. Vse države članice morajo sprejeti primerne ukrepe, s katerimi pravne osebe na območju svoje pristojnosti obvežejo k varstvu osebnih podatkov, ki jih vzdržujejo.

Predlog spremembe 12

Predlog direktive
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi morali pristojni organi vzpostaviti skupno spletišče, na katerem bi objavljali nezaupne informacije o incidentih in tveganjih.	(16) Za zagotavljanje preglednosti ter ustrezno obveščanje državljanov EU in tržnih udeležencev bi morali pristojni organi vzpostaviti skupno spletišče, na katerem bi objavljali nezaupne informacije o incidentih in tveganjih. ***Objava osebnih podatkov na tem spletišču bi morala biti omejena le na potrebne podatke in bi morala zagotoviti najvišjo možno raven anonimnosti;***

Predlog spremembe 13

Predlog direktive
Uvodna izjava 30 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(30a) Ta direktiva ne posega v pravni red Unije na področju varstva podatkov. Osebne podatke, ki se uporabijo v skladu z

določbami te direktive, bi bilo treba omejiti na najmanjši možni niz nujno potrebnih osebnih podatkov, posredovani pa bi lahko bili le tistim akterjem, za katere je to nujno potrebno, morali pa bi biti tudi karseda anonimni oz. popolnoma anonimni.

Predlog spremembe 14

Predlog direktive
Uvodna izjava 32 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(32a) Veljavna direktiva (direktiva o varnosti omrežij) ne posega v nujno potrebno sprejemanje zakonodaje EU o splošnem varstvu podatkov.

Predlog spremembe 15

Predlog direktive
Uvodna izjava 34 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(34a) Na ravni EU je treba urediti prodajo, nabavo, prenos ali izvoz opreme ali programske opreme, namenjene predvsem spremljanju ali prestrezanju interneta in telefonskega sporočanja prek mobilnega ali fiksnega omrežja, v tretje države ter zagotavljanje pomoči pri namestitvi, upravljanju ali posodabljanju te opreme ali programske opreme. Komisija mora čim prej pripraviti zakonodajo, ki bo evropskim podjetjem preprečila izvoz tega blaga z dvojno rabo nedemokratičnim, avtoritarnim in represivnim režimom.

Predlog spremembe 16

Predlog direktive
Člen 1 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno ***in*** učinkovito obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme;	(b) vzpostavlja mehanizem za sodelovanje med državami članicami, da se zagotovi enotna uporaba te direktive v Uniji ter po potrebi usklajeno***,*** učinkovito ***in uspešno*** obravnavanje in odzivanje na tveganja in incidente, ki vplivajo na omrežja in informacijske sisteme;

Predlog spremembe 17

Predlog direktive
Člen 3 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) vsako ***napravo ali*** skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo računalniških podatkov ter	(b) vsako skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo računalniških podatkov***,*** ter

Predlog spremembe 18

Predlog direktive
Člen 3 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	a) „kibernetska odpornost“ pomeni zmožnost omrežnega in informacijskega sistema, da vzdrži in obnovi polno operativno zmogljivost po incidentih, med drugim po tehnični motnji, izpadu energije ali varnostnem incidentu;

Predlog spremembe 19

Predlog direktive
Člen 3 – odstavek 8 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) upravljavca kritične infrastrukture, ki je bistvena za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energetike, prometa, bančništva, borze ***in*** zdravja;	(b) upravljavca kritične infrastrukture, ki je bistvena za vzdrževanje ključnih gospodarskih in družbenih dejavnosti na področjih energetike, prometa, bančništva, borze***,*** zdravja***, varnosti in obrambe***; ***Priloga II vsebuje neizčrpen seznam takih upravljavcev;***

Predlog spremembe 20

Predlog direktive
Člen 3 – odstavek 8 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) ponudnika naprav, omrežij in informacijskih sistemov iz točke (1) ali njihovih sestavnih delov, ki so nujni za visoko raven skupne varnosti omrežij in informacij;

Predlog spremembe 21

Predlog direktive
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica določi nacionalni organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).	1. Vsaka država članica določi ***civilni*** nacionalni organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).

Predlog spremembe 22

Predlog direktive

Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica ustanovi skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I**.** CERT se lahko ustanovi znotraj pristojnega organa.	1. Vsaka država članica ustanovi ***vsaj eno*** skupino za odzivanje na računalniške grožnje (v nadaljnjem besedilu: CERT), ki je odgovorna za obvladovanje incidentov in tveganj po natančno določenem poteku ter izpolnjuje zahteve iz točke (1) Priloge I CERT se lahko ustanovi znotraj pristojnega organa.

Predlog spremembe 23

Predlog direktive
Člen 8 – odstavek 3 – točka f a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(fa) če je to primerno glede na naravo tveganja ali grožnje, v obliki poročila obvestijo koordinatorja EU za boj proti terorizmu in so lahko naprošeni, naj z analizo pomagajo pri pripravljalnih delih in dejavnostih mreže za sodelovanje;

Predlog spremembe 24

Predlog direktive
Člen 9 – odstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	1a. Osebni podatki se razkrijejo le prejemnikom, ki morajo te podatke obdelati v okviru opravljanja svojih nalog v skladu z ustrezno pravno podlago. Razkriti podatki so omejeni na to, kar je nujno za opravljanje njihovih nalog. Zagotovi se upoštevanje načela omejitve namena. Časovna omejitev hrambe teh podatkov se določi za namene, določene v tej direktivi.

Predlog spremembe 25

Predlog direktive
Člen 10 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Na zahtevo države članice ali na lastno pobudo lahko Komisija od države članice zahteva, da zagotovi vse ustrezne informacije o določenem tveganju ali incidentu.	3. Na zahtevo države članice ali na lastno pobudo lahko Komisija od države članice zahteva, da zagotovi vse ustrezne informacije o določenem tveganju ali incidentu ***v skladu z določbami uredbe o splošnem varstvu podatkov***.

Predlog spremembe 26

Predlog direktive
Člen 13 – odstavek -1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(-1a) Visoki predstavnik Unije za zunanje zadeve in varnostno politiko in podpredsednik Komisije vključi vidike kibernetske varnosti v zunanje delovanje EU (zlasti odnose s tretjimi državami). Cilj je okrepiti izmenjavo pridobljenih izkušenj in sodelovanje pri vprašanjih kibernetske varnosti.

Predlog spremembe 27

Predlog direktive
Člen 13 – odstavek -1 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(-1b) Svet in Komisija v okviru svojih odnosov in sporazumov o sodelovanju s tretjimi državami, zlasti tistimi, pri katerih gre za sodelovanje na področju tehnologije, vztrajata pri minimalnih standardih varnosti informacijskih sistemov.

Predlog spremembe 28

Predlog direktive
Člen 20 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Pregled	***Poročanje in*** pregled

Predlog spremembe 29

Predlog direktive
Člen 20 – odstavek -1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(-1a) Komisija Evropskemu parlamentu in Svetu predloži letno poročilo o incidentih in ukrepih, o katerih je obveščena v skladu s to direktivo.

Predlog spremembe 30

Predlog direktive
Priloga 1 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) CERT izvajajo in upravljajo varnostne ukrepe, s čimer zagotovijo zaupnost, celovitost, razpoložljivost in verodostojnost informacij, ki jih prejmejo in obravnavajo.	(b) CERT izvajajo in upravljajo varnostne ukrepe, s čimer zagotovijo zaupnost, celovitost, razpoložljivost in verodostojnost informacij, ki jih prejmejo in obravnavajo***, ob spoštovanju zahtev glede varstva podatkov***.

Predlog spremembe 31

Predlog direktive
PRILOGA II – drugi podnaslov (iz člena 3(8) b) – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(5a) Obrambni in varnostni sektor:

gospodarski subjekti za dela in storitve iz Direktive 2009/81/ES, zlasti tisti iz člena 46 navedene direktive.

POSTOPEK

Naslov	Visoka skupna raven varnosti omrežij in informacij v Uniji
Referenčni dokumenti	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Pristojni odbor Datum razglasitve na zasedanju	IMCO 15.4.2013
Mnenje pripravil Datum razglasitve na zasedanju	AFET 15.4.2013
Pripravljavec/-ka mnenja Datum imenovanja	Ana Gomes 19.2.2013
Obravnava v odboru	18.9.2013
Datum sprejetja	5.12.2013
Izid končnega glasovanja	+: 31 –: 3 0: 8
Poslanci, navzoči pri končnem glasovanju	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marieta Gianaku (Marietta Giannakou), Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrej Kovačev (Andrey Kovatchev), Eduard Kukan, Marusja Ljubčeva (Marusya Lyubcheva), Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
Namestniki, navzoči pri končnem glasovanju	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
Namestniki (člen 187(2)), navzoči pri končnem glasovanju	Hiltrud Breyer

POSTOPEK

Naslov	Visoka skupna raven varnosti omrežij in informacij v Uniji			
Referenčni dokumenti	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Datum predložitve EP	5.2.2013			
Pristojni odbor Datum razglasitve na zasedanju	IMCO 15.4.2013			
Odbori, zaprošeni za mnenje Datum razglasitve na zasedanju	AFET 15.4.2013	INTA 15.4.2013	BUDG 15.4.2013	ECON 15.4.2013
	ENVI 15.4.2013	ITRE 15.4.2013	TRAN 15.4.2013	JURI 15.4.2013
	LIBE 15.4.2013			
Odbori, ki niso podali mnenja Datum sklepa	INTA 20.3.2013	BUDG 21.2.2013	ECON 18.6.2013	ENVI 19.2.2013
	TRAN 18.3.2013	JURI 20.2.2013		
Pridruženi odbori Datum razglasitve na zasedanju	ITRE 12.9.2013	LIBE 12.9.2013		
Poročevalec/-ka Datum imenovanja	Andreas Schwab 20.3.2013			
Obravnava v odboru	25.4.2013	18.6.2013	5.9.2013	4.11.2013
	9.1.2014			
Datum sprejetja	23.1.2014			
Izid končnega glasovanja	+: –: 0:	33 1 1		
Poslanci, navzoči pri končnem glasovanju	Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borisov (Preslav Borissov), Sergio Gaetano Cofferati, Lara Comi, Anna Maria Corazza Bildt, Christian Engström, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Małgorzata Handzlik, Eduard-Raul Hellvig, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Franz Obermayr, Sirpa Pietikäinen, Zuzana Roithová, Heide Rühle, Andreas Schwab, grofica Róża Thun Und Hohenstein, Bernadette Vergnaud, Barbara Weiler			
Namestniki, navzoči pri končnem glasovanju	Regina Bastos, Ashley Fox, María Irigoyen Pérez, Morten Løkkegaard, Tadeusz Ross, Marc Tarabella, Patricia van der Kammen, Sabine Verheyen, Josef Weidenholzer			
Namestniki (člen 187(2)), navzoči pri končnem glasovanju	Vital Moreira, Oreste Rossi			
Datum predložitve	12.2.2014			