Evropski parlament
2019-2024

Odbor za zunanje zadeve

2020/0359(COD)

15.7.2021

MNENJE

Odbora za zunanje zadeve

za Odbor za industrijo, raziskave in energetiko

o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Pripravljavka mnenja: Markéta Gregorová

PA_Legam

PREDLOGI SPREMEMB

Odbor za zunanje zadeve poziva Odbor za industrijo, raziskave in energetiko kot pristojni odbor, da upošteva naslednje predloge sprememb:

Predlog spremembe 1

Predlog direktive
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Od začetka veljavnosti Direktive (EU) 2016/1148 je bil dosežen velik napredek pri zviševanju ravni kibernetske odpornosti v Uniji. Pregled navedene direktive je pokazal, da se je uporabljala kot katalizator za institucionalni in regulativni pristop h kibernetski varnosti v Uniji, s čimer je utrla pot do velike spremembe v mišljenju. Direktiva je zagotovila dokončanje nacionalnih okvirov z opredelitvijo nacionalnih strategij za kibernetsko varnost, vzpostavitvijo nacionalnih zmogljivosti in izvajanjem regulativnih ukrepov, ki so zajemali bistvene infrastrukture in akterje, ki so jih določile posamezne države članice. Prispevala je tudi k sodelovanju na ravni Unije z ustanovitvijo skupine za sodelovanje[12] in mreže nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT)[13]. Kljub navedenim dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetske varnosti.	(2) Od začetka veljavnosti Direktive (EU) 2016/1148 je bil dosežen velik napredek pri zviševanju ravni kibernetske odpornosti v Uniji. Pregled navedene direktive je pokazal, da se je uporabljala kot katalizator za institucionalni in regulativni pristop h kibernetski varnosti v Uniji, s čimer je utrla pot do velike spremembe v mišljenju. Direktiva je zagotovila dokončanje nacionalnih okvirov z opredelitvijo nacionalnih strategij za kibernetsko varnost, vzpostavitvijo nacionalnih zmogljivosti in izvajanjem regulativnih ukrepov, ki so zajemali bistvene infrastrukture in akterje, ki so jih določile posamezne države članice. Prispevala je tudi k sodelovanju na ravni Unije z ustanovitvijo skupine za sodelovanje[12] in mreže nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT)[13]. ***Direktiva (EU) 2016/1148 je bila prvi zakonodajni akt o kibernetski varnosti, ki velja za vso Unijo in ki tudi na področju varnosti in obrambe določa pravne ukrepe za višjo splošno raven kibernetske odpornosti v Uniji, tako da omogoča sodelovanje držav članic in kulturo varnosti v različnih sektorjih.*** Kljub navedenim dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetske varnosti***, ki se pogosto pojavljajo zunaj Unije,***

vendar resno ogrožajo notranjo in zunanjo varnost na ravni Unije.

[12] Člen 11 Direktive (EU) 2016/1148.

[13] Člen 12 Direktive (EU) 2016/1148.

[12] Člen 11 Direktive (EU) 2016/1148.

[13] Člen 12 Direktive (EU) 2016/1148.

Predlog spremembe 2

Predlog direktive
Uvodna izjava 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) Hibridne kampanje so po pojmovanju Unije „večdimenzionalne ter združujejo prisilne in subverzivne ukrepe, pri čemer uporabljajo konvencionalna in nekonvencionalna orodja in taktike (diplomatske, vojaške, ekonomske in tehnološke) za destabilizacijo nasprotnika. Zasnovane so tako, da jih je težko odkriti ali pripisati nekomu, uporabljajo pa jih lahko državni in nedržavni akterji.“[1a]. Z internetom in spletnimi omrežji imajo državni in nedržavni akterji nove možnosti za agresivne ukrepe. Uporabijo jih lahko za vdiranje v kritično infrastrukturo in demokratične procese, uvajanje prepričljivih dezinformacijskih in propagandnih kampanj, krajo informacij in objavljanje občutljivih podatkov. V najhujšem primeru kibernetski napadi nasprotniku omogočijo, da prevzame nadzor nad sredstvi, kot so vojaški sistemi in strukture poveljevanja[1b]. Hkrati je odločilno sodelovanje z zasebnim sektorjem in civilnimi deležniki, tudi sektorji in subjekti, ki upravljajo kritične infrastrukture, in bi ga bilo treba poglobiti zaradi posebnih značilnosti kibernetske domene, kjer inovacije večinoma prispevajo zasebna podjetja, ki pa pogosto ne delujejo na vojaškem področju; Na takšne kibernetske incidente in krize velikega obsega na ravni Unije se je treba ustrezno pripraviti in se pred njimi zavarovati s pomočjo skupnih urjenj, saj

je mogoče sklicevanje na člen 222 PDEU (solidarnostna klavzula).

[1a] Evropska komisija/visoki predstavnik Unije za zunanje zadeve in varnostno politiko, „Skupno sporočilo o povečanju odpornosti in krepitvi zmogljivosti za obravnavanje hibridnih groženj“, JOIN(2018) 16 final, Bruselj, 13. junija 2018, str. 1.

[1b]

https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Predlog spremembe 3

Predlog direktive
Uvodna izjava 3 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3b) Med kibernetskimi incidenti in krizami velikega obsega na ravni Unije je zaradi visoke stopnje medsebojne odvisnosti sektorjev in držav potrebno usklajeno ukrepanje, ki bo omogočilo hiter in učinkovit odziv ter boljše preprečevanje podobnih razmer in pripravljenost nanje v prihodnosti. Razpoložljivost kibernetsko odpornih omrežij in informacijskih sistemov ter razpoložljivost, zaupnost in celovitost podatkov so ključnega pomena za varnost Unije znotraj in zunaj njenih meja. Za ambicijo Unije, da pridobi vidnejšo geopolitično vlogo, sta pomembna tudi verodostojna kibernetska obramba in odvračanje, vključno z zmožnostjo pravočasnega učinkovitega prepoznavanja zlonamernih dejanj in ustreznega odzivanja. Ker so meje med civilnimi in vojaškimi zadevami zabrisane in zaradi dvojne rabe kibernetskih orodij in tehnologij je potreben celovit in celosten pristop k digitalnemu področju. To velja tudi za operacije in misije skupne varnostne in obrambne politike (SVOP),

ki jih Unija izvaja, da bi zagotovila mir in stabilnost v svojem sosedstvu in širše. Strateški kompas EU bi moral v zvezi s tem okrepiti in usmerjati uresničevanje ravni ambicij Unije na področju varnosti in obrambe ter te ambicije pretvoriti v potrebe po zmogljivostih na področju kibernetske obrambe, s čimer bi se povečala sposobnost Unije in držav članic za preprečevanje zlonamernih kibernetskih dejavnosti, odvračanje od njih, odzivanje nanje in okrevanje po njih s krepitvijo drže, situacijskega zavedanja, orodij, postopkov in partnerstev. Sodelovanje Unije z mednarodnimi organizacijami, kot je NATO, prispeva k razpravam o tem, kako preprečevati hibridne in kibernetske napade, jih odvračati in se nanje odzivati, pa tudi kako raziskati načine za vzpostavitev skupne analize kibernetskih groženj.

Predlog spremembe 4

Predlog direktive
Uvodna izjava 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(6) Ta direktiva ne vpliva na zmožnost držav članic, da sprejmejo potrebne ukrepe, s katerimi zaščitijo bistvene interese svoje varnosti, javni red in javno varnost ter omogočijo preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. V skladu s členom 346 PDEU nobena država članica ni dolžna dajati informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene javne varnosti. V tem smislu so pomembni nacionalna pravila in pravila Unije za varovanje tajnih podatkov, sporazumi o nerazkritju informacij ali neuradni sporazumi o nerazkritju informacij, kot je semaforski protokol (Traffic Light Protocol)[14].	(6) Ta direktiva ne vpliva na zmožnost držav članic, da sprejmejo potrebne ukrepe, s katerimi zaščitijo bistvene interese svoje varnosti, javni red in javno varnost ter omogočijo preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije ***in temeljnimi pravicami. Ne glede na tehnološko okolje je nujno v celoti spoštovati predpisane postopke ter druge zaščitne ukrepe in temeljne pravice, zlasti pravico do spoštovanja zasebnega življenja in komunikacij ter pravico do varstva osebnih podatkov. Podobno je treba za zagotovitev celovite odpornosti ne le okrepiti tehnološko infrastrukturo in imeti na voljo zmogljivosti za odzivanje, temveč tudi bolje seznaniti javnost s kibernetskim tveganjem in varnostjo.*** V skladu s členom 346 PDEU nobena država

članica ni dolžna dajati informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene javne varnosti. V tem smislu so pomembni nacionalna pravila in pravila Unije za varovanje tajnih podatkov, sporazumi o nerazkritju informacij ali neuradni sporazumi o nerazkritju informacij, kot je semaforski protokol (Traffic Light Protocol)[14].

[14] Semaforski protokol je sredstvo, s katerim nekdo, ki izmenjuje informacije, obvesti svoje ciljne skupine o morebitnih omejitvah pri nadaljnjem širjenju teh informacij. Uporablja se v skoraj vseh skupnostih CSIRT ter nekaterih centrih za izmenjavo in analizo informacij.

[14] Semaforski protokol je sredstvo, s katerim nekdo, ki izmenjuje informacije, obvesti svoje ciljne skupine o morebitnih omejitvah pri nadaljnjem širjenju teh informacij. Uporablja se v skoraj vseh skupnostih CSIRT ter nekaterih centrih za izmenjavo in analizo informacij.

Predlog spremembe 5

Predlog direktive
Uvodna izjava 14 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(14a) Da bi razvili sistem varne povezljivosti, pri čemer bi se opirali na evropsko infrastrukturo za kvantno komunikacijo (EuroQCI) in vladno satelitsko komunikacijo Evropske unije (GOVSATCOM), zlasti pa začeli izvajati vodilni program Galileo/GNSS za uporabnike na področju obrambe, bi morali pri vsem morebitnem prihodnjem razvoju med drugim upoštevati učinek združitve hitrosti in izpopolnjenosti kvantnega računalništva in zelo avtonomnih vojaških sistemov, zato morajo države članice zagotoviti zaščito celotne infrastrukture za elektronsko komuniciranje, kot so vesoljska, kopenska in podmorska omrežja. Hkrati bi bilo treba oblikovati skupno strategijo sprejemanja računalništva v oblaku za občutljive sektorje, da bi opredelili pristop Unije na osnovi skupnih standardov

podobno mislečih držav.

Predlog spremembe 6

Predlog direktive
Uvodna izjava 20

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(20) Navedene vse večje medsebojne odvisnosti so rezultat vse bolj čezmejne in medsebojno odvisne mreže opravljanja storitev z uporabo ključnih infrastruktur po vsej Uniji v sektorjih energije, prometa, digitalne infrastrukture, pitne in odpadne vode, zdravja, nekaterih vidikov javne uprave in vesolja, kar zadeva opravljanje nekaterih storitev, ki so odvisne od talne infrastrukture, ki jih imajo v lasti, jih upravljajo in vodijo bodisi države članice bodisi zasebni subjekti, s čimer torej niso zajete infrastrukture, ki jih ima v lasti, jih upravlja ali vodi Unija ali ki so v lasti, se upravljajo ali vodijo v imenu Unije v okviru njenih vesoljskih programov. Te medsebojne odvisnosti pomenijo, da ima lahko kakršna koli motnja, tudi takšna, ki je prvotno omejena na en subjekt ali en sektor, širše kaskadne učinke, ki imajo lahko daljnosežne in dolgotrajne negativne učinke na opravljanje storitev na notranjem trgu. Pandemija COVID-19 je razkrila šibko točko naših vse bolj medsebojno odvisnih družb zaradi tveganj z majhno verjetnostjo.	(20) Navedene vse večje medsebojne odvisnosti so rezultat vse bolj čezmejne in medsebojno odvisne mreže opravljanja storitev z uporabo ključnih infrastruktur po vsej Uniji v sektorjih energije, prometa, digitalne infrastrukture, pitne in odpadne vode, zdravja, nekaterih vidikov javne uprave in vesolja, kar zadeva opravljanje nekaterih storitev, ki so odvisne od talne infrastrukture, ki jih imajo v lasti, jih upravljajo in vodijo bodisi države članice bodisi zasebni subjekti, s čimer torej niso zajete infrastrukture, ki jih ima v lasti, jih upravlja ali vodi Unija ali ki so v lasti, se upravljajo ali vodijo v imenu Unije v okviru njenih vesoljskih programov. ***Infrastruktura, ki je v lasti Unije ali jo Unija vodi ali z njo upravlja oziroma se vodi ali se jo upravlja v imenu Unije kot del njenih vesoljskih programov, je zlasti pomembna za varnost Unije in njenih držav članic ter pravilno delovanje misij Unije v okviru SVOP. Tovrstno infrastrukturo je treba ustrezno varovati, kot to določa Uredba (EU) 2021/696 Evropskega parlamenta in Sveta[18a].*** Te medsebojne odvisnosti pomenijo, da ima lahko kakršna koli motnja, tudi takšna, ki je prvotno omejena na en subjekt ali en sektor, širše kaskadne učinke, ki imajo lahko daljnosežne in dolgotrajne negativne učinke na opravljanje storitev na notranjem trgu ***ter ogrožajo varnost državljanov Unije.*** Pandemija COVID-19 je razkrila šibko točko naših vse bolj medsebojno odvisnih družb zaradi tveganj z majhno verjetnostjo.

_____

[18a]Uredba (EU) 2021/696 Evropskega parlamenta in Sveta z dne 28. aprila 2021 o vzpostavitvi Vesoljskega programa Unije in ustanovitvi Agencije Evropske unije za vesoljski program ter razveljavitvi uredb (EU) št. 912/2010, (EU) št. 1285/2013 in (EU) št. 377/2014 in Sklepa št. 541/2014/EU (UL L 170, 12.5.2021, str. 69).

Predlog spremembe 7

Predlog direktive
Uvodna izjava 26

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(26) Mednarodno sodelovanje na področju kibernetske varnosti je pomembno, zato bi morali skupinam CSIRT poleg sodelovanja v mreži skupin CSIRT, vzpostavljeni s to direktivo, omogočiti sodelovanje tudi v mrežah mednarodnega sodelovanja.	(26) Mednarodno sodelovanje na področju kibernetske varnosti je pomembno, zato bi morali skupinam CSIRT poleg sodelovanja v mreži skupin CSIRT, vzpostavljeni s to direktivo, omogočiti sodelovanje tudi v mrežah mednarodnega sodelovanja***, da bi prispevali k oblikovanju standardov Unije, ki lahko sooblikujejo krajino kibernetske varnosti na mednarodni ravni. Države članice bi lahko preučile tudi možnost povečanja sodelovanja s podobno mislečimi partnerskimi državami in mednarodnimi organizacijami, kot so Svet Evrope, Nato, Organizacija za gospodarsko sodelovanje in razvoj, Organizacija za varnost in sodelovanje v Evropi ter Organizacija združenih narodov, da bi sklenile večstranske sporazume o kibernetskih normah, odgovornem državnem in nedržavnem ravnanju v kibernetskem prostoru in učinkovitem svetovnem digitalnem upravljanju ter vzpostavile odprt, svoboden, stabilen in varen kibernetski prostor, ki bo temeljil na mednarodnem pravu.***

Predlog spremembe 8

Predlog direktive

Uvodna izjava 27

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(27) V skladu s Prilogo k Priporočilu Komisije (EU) 2017/1548 o usklajenem odzivu na velike kibernetske incidente in krize („načrt“)[20] bi moral velik incident pomeniti incident, ki ima velik vpliv na vsaj dve državi članici ali ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje. Glede na njihov vzrok in vpliv se lahko veliki incidenti stopnjujejo in sprevržejo v popolno krizo, ki ne omogoča ustreznega delovanja notranjega trga. Glede na velik obseg in večinoma čezmejno naravo takih incidentov bi morali države članice ter ustrezne institucije, organi in agencije Unije sodelovati na tehnični, operativni in politični ravni za ustrezno usklajevanje odziva po vsej Uniji.	(27) V skladu s Prilogo k Priporočilu Komisije (EU) 2017/1548 o usklajenem odzivu na velike kibernetske incidente in krize („načrt“)[20] bi moral velik incident pomeniti incident, ki ima velik vpliv na vsaj dve državi članici ali ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje. Glede na njihov vzrok in vpliv se lahko veliki incidenti stopnjujejo in sprevržejo v popolno krizo, ki ne omogoča ustreznega delovanja notranjega trga ***ali ogrožajo varnost državljanov ter gospodarske in finančne interese Unije.*** Glede na velik obseg in večinoma čezmejno naravo takih incidentov bi morali države članice ter ustrezne institucije, organi in agencije Unije sodelovati na tehnični, operativni in politični ravni za ustrezno usklajevanje odziva po vsej Uniji. ***Unija in države članice pa bi morale nadalje spodbujati tudi politične razprave o okviru kriznega upravljanja na podlagi vaj in scenarijev, da bi zagotovile skladnost notranje in zunanje politike ter oblikovale skupno razumevanje postopkov za izvajanje solidarnostne klavzule.***
[20] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).	[20] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

Predlog spremembe 9

Predlog direktive
Uvodna izjava 36

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(36) Unija bi morala, kjer je ustrezno, v skladu s členom 218 PDEU skleniti mednarodne sporazume s tretjimi državami	(36) Unija bi morala, kjer je ustrezno, v skladu s členom 218 PDEU skleniti mednarodne sporazume s tretjimi državami

ali mednarodnimi organizacijami, ki bi omogočali in urejali njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje in mreže skupin CSIRT. Taki sporazumi ***bi morali zagotoviti*** ustrezno varstvo podatkov.	ali mednarodnimi organizacijami, ki bi omogočali in urejali njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje in mreže skupin CSIRT. Taki sporazumi ***morajo zagotavljati*** ustrezno varstvo podatkov***, obenem pa bi morali spodbujati dostop do trga in odpravljati varnostna tveganja, izboljšati globalno odpornost ter ozaveščati o kibernetskih grožnjah in zlonamernih kibernetskih dejavnostih. Unija bi morala še naprej podpirati izgradnjo zmogljivosti v tretjih državah. Države članice bi morale po potrebi spodbujati udeležbo podobno mislečih partnerskih držav, s katerimi delijo vrednote Unije, v ustreznih projektih PESCO. Zato bi morala Unija preučiti možnost ponovne uvedbe postopkov za vzpostavitev formalnih in strukturiranih okvirov sodelovanja na tem področju v prihodnosti.***

Predlog spremembe 10

Predlog direktive
Uvodna izjava 37

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(37) Države članice bi morale prispevati k vzpostavitvi okvira EU za odzivanje na krize na področju kibernetske varnosti, določenega v Priporočilu (EU) 2017/1584, z obstoječimi mrežami za sodelovanje, zlasti organizacijsko mrežo za povezovanje v kibernetski krizi (EU-CyCLONe), mrežo skupin CSIRT in skupino za sodelovanje. Mreža EU-CyCLONe in mreža skupin CSIRT bi morali sodelovati na podlagi postopkovnih ureditev, v katerih so opredeljeni načini navedenega sodelovanja. V poslovniku mreže EU-CyCLONe bi morali biti podrobneje opredeljeni načini delovanja mreže, med drugim z vlogami, načini sodelovanja, stiki z drugimi ustreznimi akterji in predlogami za izmenjavo informacij ter sredstvi komuniciranja. Za obvladovanje krize na	(37) Države članice bi morale prispevati k vzpostavitvi okvira EU za odzivanje na krize na področju kibernetske varnosti, določenega v Priporočilu (EU) 2017/1584, z obstoječimi mrežami za sodelovanje, zlasti organizacijsko mrežo za povezovanje v kibernetski krizi (EU-CyCLONe), mrežo skupin CSIRT in skupino za sodelovanje***, Evropskim centrom za boj proti kibernetski kriminaliteti in Obveščevalnim in situacijskim centrom EU (INTCEN), da bi razširile strateško obveščevalno sodelovanje na področju kibernetskih groženj in dejavnosti, s tem pa nadalje podprle spremljanje razmer v Uniji in odločanje o skupnem diplomatskem odzivu.*** Mreža EU-CyCLONe in mreža skupin CSIRT bi morali sodelovati na podlagi postopkovnih ureditev, v katerih so

ravni Unije bi se morale ustrezne strani zanašati na enotne ureditve za politično odzivanje na krize (IPCR). Komisija bi morala v ta namen uporabljati postopek medsektorskega kriznega usklajevanja na visoki ravni v okviru sistema ARGUS. Če bo imela kriza znaten vpliv na ***zunanjo ali skupno varnostno in obrambno politiko (***SVOP***)***, bi bilo treba sprožiti mehanizem Evropske službe za zunanje delovanje (ESZD) za krizno odzivanje.

opredeljeni načini navedenega sodelovanja. V poslovniku mreže EU-CyCLONe bi morali biti podrobneje opredeljeni načini delovanja mreže, med drugim z vlogami, načini sodelovanja, stiki z drugimi ustreznimi akterji in predlogami za izmenjavo informacij ter sredstvi komuniciranja. Za obvladovanje krize na ravni Unije bi se morale ustrezne strani zanašati na enotne ureditve za politično odzivanje na krize (IPCR)***, ki podpirajo tudi politično usklajevanje odziva ob sklicevanju na uporabo solidarnostne klavzule.*** Komisija bi morala v ta namen uporabljati postopek medsektorskega kriznega usklajevanja na visoki ravni v okviru sistema ARGUS. Če bo imela kriza znaten vpliv na SVOP, bi bilo treba sprožiti mehanizem Evropske službe za zunanje delovanje (ESZD) za krizno odzivanje ***in vse druge ukrepe, s katerimi se bodo zaščitile misije in operacije v okviru skupne varnostne in obrambne politike in delegacije Unije. Poleg tega bi morala Unija v celoti izkoristiti svoj nabor orodij kibernetske diplomacije.***

Predlog spremembe 11

Predlog direktive
Uvodna izjava 40 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(40a) Države članice bi morale razmisliti o programu aktivne kibernetske obrambe, ki bi bil del njihove nacionalne strategije za kibernetsko varnost določiti, katere del bi bila redna skupna urjenja držav članic in v okviru mednarodnih organizacij, ki bi omogočal, da se sinhronizirano in v realnem času odkrivajo, preiskujejo, analizirajo in blažijo grožnje. Aktivna kibernetska obramba deluje z omrežno hitrostjo s pomočjo senzorjev, programske opreme in obveščevalnih podatkov, njen namen pa je odkrivati in preprečevati zlonamerne dejavnosti, po možnosti preden bi se lahko razširile na omrežja in

sisteme. Poleg tega bi morale države članice močno izboljšati metodo za izmenjavo informacij in opredeliti skupni komunikacijski standard, ki bi se lahko uporabljal za tajne in netajne podatke, da bi zagotovile hitro ukrepanje. Unija in države članice bi morale okrepiti tudi zmogljivosti za ugotavljanje odgovornosti za kibernetske napade, da bi jih lahko učinkovito preprečevale in se odzivale nanje na sorazmeren način v skladu z mednarodnim pravom.

Predlog spremembe 12

Predlog direktive
Uvodna izjava 40 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(40b) Države članice bi morale v svojih nacionalnih strategijah za kibernetsko varnost določiti program aktivne kibernetske obrambe. Gre za proaktivno odkrivanje, analiziranje in ublažitev kršitev varnosti omrežja v realnem času, skupaj z uporabo zmogljivosti, ki se uporabljajo zunaj mreže žrtve. Program temelji na obrambni strategiji, ki izključuje ofenzivne ukrepe proti kritični civilni infrastrukturi nasprotnikov, če bi ta pomenila kršitev mednarodnega prava (kot je dodatni protokol iz leta 1977 k ženevskim konvencijam). Sposobnost hitre in samodejne izmenjave in razumevanja informacij o grožnjah in njihove analize, pa tudi opozoril o kibernetskih dejavnostih in ukrepov za odzivanje je ključnega pomena, da bi omogočili enotna prizadevanja za uspešno odkrivanje in preprečevanje kibernetskih napadov. Dejavnosti aktivne kibernetske obrambe bi lahko vključevale konfiguracije poštnih strežnikov in spletišč, omogočanje beleženja in filtriranje sistema domenskih imen. Države članice bi morale sprejeti politike, ki bodo omogočile najširšo možno

uporabo najučinkovitejših orodij za kibernetsko varnost ter podprle mala, srednja in druga podjetja ter finančno šibka podjetja z ugodnostmi, nepovratnimi sredstvi, posojili in davčnimi ugodnostmi pri nakupu najboljših proizvodov in storitev za kibernetsko varnost, s čimer se bo preprečilo, da stroški ne bodo postali element diskriminacije. Prav tako bi si morale prizadevati za spodbujanje partnerstev z akademskimi ustanovami in drugimi raziskovalnimi središči, da bi spodbudili raziskave in razvoj na področju kibernetske varnosti ter z večdisciplinarnim pristopom razvili nove tehnologije, orodja in veščine, uporabne tako v civilnem kot obrambnem sektorju. Partnerstva bi bilo treba financirati z obstoječimi in novimi instrumenti pod okriljem Komisije.

Predlog spremembe 13

Predlog direktive
Uvodna izjava 43

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(43) Obravnavanje tveganj za kibernetsko varnost, ki izhajajo iz dobavne verige subjekta in njegovega razmerja z njegovimi dobavitelji, je še zlasti pomembno glede na razširjenost incidentov, v katerih so bili subjekti žrtve kibernetskih napadov in v katerih so bili zlonamerni akterji sposobni ogroziti varnost omrežij in informacijskih sistemov subjekta z izkoriščanjem šibkih točk, ki vplivajo na proizvode in storitve tretje osebe. Subjekti bi morali zato oceniti in upoštevati splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.	(43) Obravnavanje tveganj za kibernetsko varnost, ki izhajajo iz dobavne verige subjekta in njegovega razmerja z njegovimi dobavitelji, je še zlasti pomembno glede na razširjenost incidentov, v katerih so bili subjekti žrtve kibernetskih napadov in v katerih so bili zlonamerni akterji sposobni ogroziti varnost omrežij in informacijskih sistemov subjekta z izkoriščanjem šibkih točk, ki vplivajo na proizvode in storitve tretje osebe. Subjekti bi morali zato oceniti in upoštevati splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi ***sistemi za obvladovanje tveganja in*** varnimi razvojnimi postopki ***v skladu s standardi Unije na področju kibernetske varnosti***.

Predlog spremembe 14

Predlog direktive
Uvodna izjava 43 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(43a) Morebitni netehnični dejavniki tveganja, kot je neprimeren vpliv tretje države na dobavitelje in ponudnike storitev, zlasti v primeru alternativnih modelov upravljanja, vključujejo prikrite šibke točke ali stranska vrata in morebitne sistemske motnje v oskrbi, zlasti v primeru tehnološke vezanosti na ponudnika ali odvisnosti od njega. Ker lahko izkoriščanje šibkih točk v obrambnem sektorju povzroči hude motnje in škodo, so za kibernetsko varnost obrambne industrije potrebni posebni ukrepi, s katerimi bi zagotovili varnost dobavnih verig, zlasti subjektov, ki so nižje v dobavnih verigah in ne potrebujejo dostopa do tajnih podatkov, vendar bi lahko predstavljali resno tveganje za celotni sektor. Posebno pozornost bi morali posvetiti posledicam vsake morebitne kršitve in grožnji vsake morebitne manipulacije podatkov v omrežju, zaradi katerih bi ključna obrambna sredstva lahko postala nekoristna ali ki bi lahko celo nevtralizirala operativne sisteme, zaradi česar bi bili izpostavljeni grožnjam.

Predlog spremembe 15

Predlog direktive
Uvodna izjava 46

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(46) Za nadaljnje obravnavanje ključnih tveganj za dobavno verigo ter zagotavljanje pomoči subjektom, ki delujejo v sektorjih, zajetih s to direktivo, pri ustreznem	(46) Za nadaljnje obravnavanje ključnih tveganj za dobavno verigo ter zagotavljanje pomoči subjektom, ki delujejo v sektorjih, zajetih s to direktivo, pri ustreznem

obvladovanju tveganj za kibernetsko varnost, povezanih z dobavno verigo in dobavitelji, bi morala skupina za sodelovanje, ki vključuje ustrezne nacionalne organe, v sodelovanju s Komisijo ***in*** agencijo ENISA izvesti usklajene sektorske ocene tveganj v zvezi z dobavno verigo, kot je že storila za omrežja 5G[21] na podlagi Priporočila (EU) 2019/534 o kibernetski varnosti omrežij 5G, da bi opredelila kritične storitve, sisteme ali proizvode IKT, zadevne grožnje in šibke točke za posamezne sektorje.

obvladovanju tveganj za kibernetsko varnost, povezanih z dobavno verigo in dobavitelji, bi morala skupina za sodelovanje, ki vključuje ustrezne nacionalne organe, v sodelovanju s Komisijo***,*** agencijo ENISA ***in Evropsko službo za zunanje delovanje*** izvesti usklajene sektorske ocene tveganj v zvezi z dobavno verigo, kot je že storila za omrežja 5G[21] na podlagi Priporočila (EU) 2019/534 o kibernetski varnosti omrežij 5G, da bi opredelila kritične storitve, sisteme ali proizvode IKT, zadevne grožnje in šibke točke za posamezne sektorje.

[21] Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019 – Kibernetska varnost omrežij 5G (UL L 88, 29.3.2019, str. 42).

[21] Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019 – Kibernetska varnost omrežij 5G (UL L 88, 29.3.2019, str. 42).

Predlog spremembe 16

Predlog direktive
Uvodna izjava 68

Besedilo, ki ga predlaga Komisija

(68) Subjekte bi bilo zato treba spodbuditi, naj skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno ocenjevanje in spremljanje kibernetskih groženj, zaščito pred njimi in odzivanje nanje. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij. V ta namen bi morale države članice dejavno podpirati in spodbujati tudi ustrezne subjekte, ki niso zajeti v področje uporabe te direktive, naj sodelujejo v takih mehanizmih za izmenjavo informacij. Taki mehanizmi bi se morali izvajati ob polnem spoštovanju pravil Unije o konkurenci in pravil prava Unije o varstvu podatkov.

Predlog spremembe

(68) Subjekte bi bilo zato treba spodbuditi, naj skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno ocenjevanje in spremljanje kibernetskih groženj, zaščito pred njimi in odzivanje nanje. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij. V ta namen bi morale države članice dejavno podpirati in spodbujati tudi ustrezne subjekte, ki niso zajeti v področje uporabe te direktive, naj sodelujejo v takih mehanizmih za izmenjavo informacij. ***Poleg tega bi države članice lahko razmislile o možnosti povezovanja s podobno mislečimi partnerskimi državami.*** Taki mehanizmi bi se morali izvajati ob polnem spoštovanju pravil Unije o konkurenci in pravil prava

Unije o varstvu podatkov. ***Zato bi morale države članice podpirati pristojne organe in skupine za odzivanje na incidente na področju računalniške varnosti pri zagotavljanju brezplačne ali dostopne pomoči, izobraževanja in revizijskih programov na področju kibernetske varnosti subjektom, ki ne spadajo na področje uporabe te direktive, zlasti zagonskim podjetjem, MSP in nevladnim organizacijam.***

Predlog spremembe 17

Predlog direktive
Uvodna izjava 68 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(68a) Ker ima kibernetska varnost tako civilno kot vojaško razsežnost, bi morali spodbujati izmenjavo informacij med sektorji (obrambni, civilni, preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in zunanje delovanje). Skupna kibernetska enota bi lahko imela pomembno vlogo pri varovanju Unije pred kibernetskimi napadi, če bi akterje pomagala poučiti o grožnjah in bi usklajevala njihov odziv.

Predlog spremembe 18

Predlog direktive
Uvodna izjava 73

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(73) Kadar se upravne globe naložijo podjetjem, bi se podjetje v te namene moralo razumeti kot podjetje v skladu s členoma 101 in 102 PDEU. Kadar se upravne globe naložijo osebam, ki niso podjetje, bi moral nadzorni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe. Države	(73) Kadar se upravne globe naložijo podjetjem, bi se podjetje v te namene moralo razumeti kot podjetje v skladu s členoma 101 in 102 PDEU. Kadar se upravne globe naložijo osebam, ki niso podjetje, bi moral nadzorni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe***, brez***

članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu. Naložitev upravne globe ne vpliva na uporabo drugih pooblastil pristojnih organov ali drugih sankcij, določenih v nacionalnih pravilih, s katerimi je prenesena ta direktiva.	***poseganja v cilje te direktive***. Države članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu. Naložitev upravne globe ne vpliva na uporabo drugih pooblastil pristojnih organov ali drugih sankcij, določenih v nacionalnih pravilih, s katerimi je prenesena ta direktiva.

Predlog spremembe 19

Predlog direktive
Člen 5 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) politiko za obravnavanje kibernetske varnosti v dobavni verigi proizvodov in storitev IKT, ki jih bistveni in pomembni subjekti uporabljajo za opravljanje svojih storitev;	(a) politiko za obravnavanje kibernetske varnosti v dobavni verigi proizvodov in storitev IKT, ki jih bistveni in pomembni subjekti uporabljajo za opravljanje svojih storitev***, in sicer na podlagi celovite ocene morebitnih nevarnosti za dobavne verige;***

Predlog spremembe 20

Predlog direktive
Člen 5 – odstavek 2 – točka b a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ba) politiko za spodbujanje interoperabilnosti in spoštovanja skupnih standardov Unije na področju kibernetske varnosti;

Predlog spremembe 21

Predlog direktive
Člen 5 – odstavek 2 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) politiko, povezano z ohranjanjem splošne razpoložljivosti in celovitosti javnega jedra odprtega interneta;	(d) politiko, povezano z ohranjanjem splošne razpoložljivosti in celovitosti javnega jedra odprtega interneta***, vključno***

	s kibernetsko varnostjo podmorskih komunikacijskih kablov, kjer je potrebna;

Predlog spremembe 22

Predlog direktive
Člen 5 – odstavek 2 – točka f

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(f) politiko za podpiranje akademskih in raziskovalnih institucij pri razvoju orodij in varne omrežne infrastrukture za kibernetsko varnost;	(f) politiko za podpiranje akademskih in raziskovalnih institucij pri ***raziskavah kibernetske varnosti ter pri*** razvoju orodij in varne omrežne infrastrukture za kibernetsko varnost;

Predlog spremembe 23

Predlog direktive
Člen 5 – odstavek 2 – točka h

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(h) politiko za obravnavanje posebnih potreb MSP, zlasti tistih, ki so izključena s področja uporabe te direktive, v zvezi z usmeritvami in podporo pri povečevanju njihove odpornosti proti kibernetskim grožnjam.	(h) politiko za obravnavanje posebnih potreb ***zagonskih podjetij,*** MSP ***in nevladnih organizacij***, zlasti tistih, ki so izključeni s področja uporabe te direktive, v zvezi z usmeritvami in podporo pri povečevanju njihove odpornosti proti kibernetskim grožnjam***, odzivanju na kibernetske incidente in iskanju pomoči na področju kibernetske varnosti;***

Predlog spremembe 24

Predlog direktive
Člen 5 – odstavek 2 – točka h a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ha) politiko za spodbujanje uporabe in razvoja odprtokodne programske opreme.

Predlog spremembe 25

Predlog direktive
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka država članica imenuje eno od svojih skupin CSIRT iz člena 9 za koordinatorko za ***usklajeno*** razkrivanje šibkih točk. Imenovana skupina CSIRT deluje kot zaupanja vredna posrednica, ki po potrebi olajšuje sodelovanje med poročajočim subjektom in proizvajalcem ali ponudnikom proizvodov ali storitev IKT. Če se sporočena šibka točka nanaša na več proizvajalcev ali ponudnikov proizvodov ali storitev IKT v Uniji, imenovana skupina CSIRT vsake zadevne države članice sodeluje z mrežo skupin CSIRT.	1. Vsaka država članica imenuje eno od svojih skupin CSIRT iz člena 9 za koordinatorko za ***obvezno odgovorno*** razkrivanje šibkih točk. Imenovana skupina CSIRT deluje kot zaupanja vredna posrednica, ki po potrebi olajšuje sodelovanje med poročajočim subjektom in proizvajalcem ali ponudnikom proizvodov ali storitev IKT. Če se sporočena šibka točka nanaša na več proizvajalcev ali ponudnikov proizvodov ali storitev IKT v Uniji, imenovana skupina CSIRT vsake zadevne države članice sodeluje z mrežo skupin CSIRT.

Predlog spremembe 26

Predlog direktive
Člen 6 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Agencija ENISA razvije in vzdržuje evropski register šibkih točk. V ta namen agencija ENISA vzpostavi in vzdržuje ustrezne informacijske sisteme, politike in postopke, zlasti z namenom omogočanja pomembnim in bistvenim subjektom ter njihovim dobaviteljem omrežnih in informacijskih sistemov, da razkrijejo in evidentirajo šibke točke proizvodov in storitev IKT ter zagotovijo dostop do informacij o šibkih točkah, vsebovanih v registru, vsem zainteresiranim stranem. Register vključuje zlasti informacije, ki opisujejo šibko točko, prizadeti proizvod ali storitev IKT ter resnost šibke točke v smislu okoliščin, v katerih jo je mogoče izkoristiti, razpoložljivost povezanih popravkov ter, če popravki niso na voljo, smernice, naslovljene na uporabnike proizvodov in storitev s šibkimi točkami, o načinih za	2. Agencija ENISA razvije in vzdržuje evropski register šibkih točk. V ta namen agencija ENISA vzpostavi in vzdržuje ustrezne informacijske sisteme, politike in postopke, zlasti z namenom omogočanja pomembnim in bistvenim subjektom ter njihovim dobaviteljem omrežnih in informacijskih sistemov, da razkrijejo in evidentirajo šibke točke proizvodov in storitev IKT ter zagotovijo dostop do informacij o šibkih točkah, vsebovanih v registru, vsem zainteresiranim stranem. ***V skladu s členom 10(2) skupine CSIRT poleg pomoči za zmanjševanje tveganja omogočajo dostop do informacij o šibkih točkah, zabeleženih v evropskem registru šibkih točk, tudi subjektom, ki ne spadajo na področje uporabe te direktive, zlasti zagonskim podjetjem, MSP in nevladnim organizacijam.*** Register vključuje zlasti

zmanjšanje tveganj, ki izhajajo iz razkritih šibkih točk.

informacije, ki opisujejo šibko točko, prizadeti proizvod ali storitev IKT ter resnost šibke točke v smislu okoliščin, v katerih jo je mogoče izkoristiti, razpoložljivost povezanih popravkov ter, če popravki niso na voljo, smernice, naslovljene na uporabnike proizvodov in storitev s šibkimi točkami, o načinih za zmanjšanje tveganj, ki izhajajo iz razkritih šibkih točk.

Predlog spremembe 27

Predlog direktive
Člen 7 – odstavek 3 – točka f

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(f) nacionalni postopki in ureditve med ustreznimi nacionalnimi organi za zagotovitev učinkovitega sodelovanja države članice pri usklajenem upravljanju velikih kibernetskih incidentov in kriz na ravni Unije ter njegove podpore.	(f) nacionalni postopki in ureditve med ustreznimi nacionalnimi organi za zagotovitev učinkovitega sodelovanja države članice pri usklajenem upravljanju velikih kibernetskih incidentov in kriz na ravni Unije ter njegove podpore***, tudi odzivi na ustrezne zahteve na podlagi solidarnostne klavzule.***

Predlog spremembe 28

Predlog direktive
Člen 7 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Države članice Komisijo obvestijo o imenovanju svojih pristojnih organov iz odstavka 1 ter predložijo svoje nacionalne načrte odzivanja na kibernetske incidente in krize iz odstavka 3 v treh mesecih od zadevnega imenovanja in sprejetja navedenih načrtov. Države članice lahko iz načrta izključijo določene informacije, če in kolikor je to nujno potrebno za njihovo nacionalno varnost.	4. Države članice Komisijo obvestijo o imenovanju svojih pristojnih organov iz odstavka 1 ter predložijo svoje nacionalne načrte odzivanja na kibernetske incidente in krize iz odstavka 3 v treh mesecih od zadevnega imenovanja in sprejetja navedenih načrtov. Države članice lahko iz načrta izključijo določene informacije, če in kolikor je to nujno potrebno za njihovo nacionalno varnost. ***V primeru velikega kibernetskega incidenta in krize, ki ne prizadene samo ene države članice in je pomemben na ravni Unije, se vzpostavi***

ustrezno krizno upravljanje in vodenje. S temi strukturami se organizirajo izmenjava informacij, usklajevanje in sodelovanje s strukturami Unije za zunanjo varnost in vojaško krizno upravljanje ter organi držav članic, pristojnimi za varnost in obrambo.

Predlog spremembe 29

Predlog direktive
Člen 9 – odstavek 4 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4a. Skupine CSIRT sodelujejo z nacionalnimi institucijami, pristojnimi za ohranjanje javne varnosti, obrambe in nacionalne varnosti, ter si z njimi izmenjujejo ustrezne informacije.

Predlog spremembe 30

Predlog direktive
Člen 9 – odstavek 4 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4b. Skupine CSIRT sodelujejo ter si, brez poseganja v pravo Unije, zlasti Uredbo (EU) 2016/679, z zaupanja vrednimi tretjimi državami in mednarodnimi organizacijami izmenjujejo relevantne informacije o kibernetskih grožnjah, šibkih točkah, dobri praksi in standardih.

Predlog spremembe 31

Predlog direktive
Člen 9 – odstavek 4 c (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	4c. Skupine CSIRT brez poseganja v pravo Unije, zlasti Uredbo (EU) 2016/679,

	skupinam CSIRT ali enakovrednim strukturam v državah kandidatkah za članstvo v Uniji in drugih tretjih državah na Zahodnem Balkanu in v vzhodnem partnerstvu zagotavljajo pomoč na področju kibernetske varnosti.

Predlog spremembe 32

Predlog direktive
Člen 10 – odstavek 2 – točka e a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ea) subjektom, ki ne spadajo na področje uporabe te direktive, zlasti zagonskim podjetjem, MSP in nevladnim organizacijam, se zagotovijo brezplačna ali dostopna pomoč, izobraževanje in revizijski programi na področju kibernetske varnosti;

Predlog spremembe 33

Predlog direktive
Člen 11 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Če je to potrebno za učinkovito opravljanje nalog in izpolnjevanje obveznosti, določenih v tej direktivi, države članice zagotovijo ustrezno sodelovanje med pristojnimi organi, enotnimi kontaktnimi točkami, organi kazenskega pregona, organi za varstvo podatkov in organi, pristojnimi za kritično infrastrukturo v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], ter nacionalnimi finančnimi organi, imenovanimi v skladu z Uredbo (EU) XXXX/XXXX Evropskega parlamenta in Sveta[39] [uredba o digitalni operativni odpornosti] v zadevni državi članici.	4. Če je to potrebno za učinkovito opravljanje nalog in izpolnjevanje obveznosti, določenih v tej direktivi, države članice zagotovijo ustrezno sodelovanje med pristojnimi organi, enotnimi kontaktnimi točkami, organi kazenskega pregona, organi za varstvo podatkov, ***nacionalnimi nadzornimi organi za umetno inteligenco, nacionalnimi pristojnimi organi za upravljanje podatkov,*** in organi, pristojnimi za kritično infrastrukturo v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], ter nacionalnimi finančnimi organi, imenovanimi v skladu z Uredbo (EU) XXXX/XXXX Evropskega parlamenta in Sveta[39] [uredba o digitalni

operativni odpornosti] v zadevni državi članici.

[39] [vstaviti polni naslov in sklic na objavo v UL, ko bosta znana].

[39] [vstaviti polni naslov in sklic na objavo v UL, ko bosta znana].

Predlog spremembe 34

Predlog direktive
Člen 12 – odstavek 3 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije ***in*** agencije ENISA. Evropska služba za zunanje delovanje sodeluje pri dejavnostih skupine za sodelovanje kot opazovalka. ***Evropski nadzorni organi lahko*** v skladu s členom 17(5)(c) Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti] ***sodelujejo pri dejavnostih skupine za sodelovanje.***	3. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije, ***EU – CyCLONe,*** agencije ENISA ***in Evropske obrambne agencije.*** Evropska služba za zunanje delovanje sodeluje pri dejavnostih skupine za sodelovanje kot opazovalka. ***Pri dejavnostih skupine za sodelovanje*** v skladu s členom 17(5)(c) Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti] sodelujejo ***tudi nacionalni nadzorni organi za umetno inteligenco, nacionalni pristojni organi za upravljanje podatkov in evropski nadzorni organi.***

Predlog spremembe 35

Predlog direktive
Člen 12 – odstavek 4 – točka e a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ea) sodelovanje, medsebojna pomoč ter izmenjava dobre prakse in informacij z zaupanja vrednimi tretjimi državami in mednarodnimi organizacijami, brez poseganja v pravo Unije;

Predlog spremembe 36

Predlog direktive
Člen 13 – odstavek 3 – točka k

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(k) sodelovanje in izmenjava informacij s centri za varnostne operacije na regionalni ravni in ravni Unije za izboljšanje skupnega situacijskega zavedanja na področju incidentov in groženj po vsej Uniji;	(k) sodelovanje in izmenjava informacij s centri za varnostne operacije na regionalni ravni in ravni Unije, ***po potrebi pa tudi z vojaškimi skupinami za odzivanje na računalniške grožnje (CERT),*** za izboljšanje skupnega situacijskega zavedanja na področju incidentov in groženj po vsej Uniji;

Predlog spremembe 37

Predlog direktive
Člen 14 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Mreža EU-CyCLONe je sestavljena iz predstavnikov organov držav članic za krizno upravljanje, imenovanih v skladu s členom 7, Komisije in agencije ENISA. Agencija ENISA zagotovi sekretariat mreže in podpira varno izmenjavo informacij.	2. Mreža EU-CyCLONe je sestavljena iz predstavnikov organov držav članic za krizno upravljanje, imenovanih v skladu s členom 7, Komisije, ***Evropske službe za zunanje delovanje*** in agencije ENISA. Agencija ENISA zagotovi sekretariat mreže in podpira varno izmenjavo informacij. ***Tem nacionalnim organom za krizno upravljanje svetuje svetovalna skupina civilne družbe. Za velike kibernetske incidente in krize, ki ne prizadenejo samo ene države članice, se vzpostavi struktura za krizno upravljanje na ravni Unije, pri kateri sodelujejo vsi ustrezni akterji. V njej so skupna kibernetska enota, skupine CSIRT, mreža skupin CSIRT, skupina za sodelovanje, Komisija, Evropska služba za zunanje delovanje in agencija ENISA. Struktura tudi pripravi in izvaja sklicevanje na solidarnostno klavzulo in njeno uporabo.***

Predlog spremembe 38

Predlog direktive
Člen 14 – odstavek 3 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) zviševanje ravni pripravljenosti za upravljanje velikih incidentov in kriz;	(a) zviševanje ravni pripravljenosti za upravljanje velikih incidentov in kriz ***in sodelovanje z agencijami držav članic, odgovornimi za državno varnost in teritorialno obrambo;***

Predlog spremembe 39

Predlog direktive
Člen 17 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Države članice zagotovijo, da se člani upravnega organa redno udeležujejo posebnih usposabljanj, da pridobijo dovolj znanja in spretnosti za razumevanje in ocenjevanje tveganj za kibernetsko varnost ter praks upravljanja in njihovega vpliva na dejavnosti subjekta.	2. Države članice zagotovijo, da se člani upravnega organa redno udeležujejo posebnih usposabljanj, da pridobijo dovolj znanja in spretnosti za razumevanje in ocenjevanje tveganj za kibernetsko varnost ter praks upravljanja in njihovega vpliva na dejavnosti subjekta. ***Države članice spodbujajo bistvene in pomembne subjekte, da pri članih upravnih organov iz odstavka 1 tega člena redno ocenjujejo ustreznost znanj in spretnosti za zagotavljanje skladnosti s členom 18.***

Predlog spremembe 40

Predlog direktive
Člen 18 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz točke (d) odstavka 2 upoštevajo šibke točke posameznega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.	3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz točke (d) odstavka 2 upoštevajo šibke točke posameznega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki ***v skladu s standardi in zakoni Unije na področju kibernetske varnosti ter morebitnimi netehničnimi dejavniki tveganja, kot so***

	prikrite šibke točke ali stranska vrata in morebitne sistemske motnje v oskrbi.

Predlog spremembe 41

Predlog direktive
Člen 19 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Skupina za sodelovanje lahko v sodelovanju s Komisijo ***in*** agencijo ENISA izvaja usklajene ocene tveganja za varnost specifičnih kritičnih storitev IKT, sistemov IKT ali dobavnih verig proizvodov IKT, ob upoštevanju tehničnih in po potrebi netehničnih dejavnikov tveganja.	1. Skupina za sodelovanje lahko v sodelovanju s Komisijo***,*** agencijo ENISA ***in Evropsko službo za zunanje delovanje*** izvaja usklajene ocene tveganja za varnost specifičnih kritičnih storitev IKT, sistemov IKT ali dobavnih verig proizvodov IKT, ob upoštevanju tehničnih in po potrebi netehničnih dejavnikov tveganja.

Predlog spremembe 42

Predlog direktive
Člen 19 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Komisija po posvetovanju s skupino za sodelovanje ***in*** agencijo ENISA opredeli specifične kritične storitve, sisteme ali proizvode IKT, ki so lahko predmet usklajene ocene tveganja iz odstavka 1.	2. Komisija po posvetovanju s skupino za sodelovanje***,*** agencijo ENISA ***in Evropsko službo za zunanje delovanje*** opredeli specifične kritične storitve, sisteme ali proizvode IKT, ki so lahko predmet usklajene ocene tveganja iz odstavka 1.

Predlog spremembe 43

Predlog direktive
Člen 19 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Komisija po opredelitvi tveganj za posamezne kritične storitve, sisteme ali proizvodne dobavne verige IKT po posvetovanju s skupino za sodelovanje, agencijo ENISA in Evropsko službo za

zunanje delovanje za države članice in pristojne nacionalne organe, opredeljene v tej uredbi, izda priporočila za odpravo ugotovljenih tveganj in povečanje odpornosti nanje.

Predlog spremembe 44

Predlog direktive
Člen 25 – odstavek 1 – točka c a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ca) informacije o upravnem organu, pristojnem za ukrepe za obvladovanje tveganj na področju kibernetske varnosti iz člena 18 v skladu s členom 17;

Predlog spremembe 45

Predlog direktive
Člen 29 – odstavek 2 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;	(c) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju***, vključno s tveganjem, povezanim z dobavnimi verigami, kot je opredeljeno v členu 18(3);***

Predlog spremembe 46

Predlog direktive
Člen 30 – odstavek 2 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;	(b) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju***, vključno s tveganjem, povezanim z dobavnimi verigami, kot je opredeljeno v členu 18(3);***

Predlog spremembe 47

Predlog direktive
Priloga I – bistveni subjekti: sektorji, podsektorji in vrste subjektov – sektor 6 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	6a. Izobraževanje in raziskave – Visokošolske in raziskovalne ustanove

Predlog spremembe 48

Predlog direktive
Priloga I – BISTVENI SUBJEKTI: SEKTORJI, PODSEKTORJI IN VRSTE SUBJEKTOV – sektor 9 Javna uprava – vrste subjektov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
– subjekti javne uprave enot centralne ravni držav	– subjekti javne uprave enot centralne ravni držav
– subjekti javne uprave regij na ravni NUTS 1, navedeni v Prilogi I k Uredbi (ES) št. 1059/2003 ([27])	– subjekti javne uprave regij na ravni NUTS 1, navedeni v Prilogi I k Uredbi (ES) št. 1059/2003 ([27], ***27 a (novo)***)
– subjekti javne uprave regij na ravni NUTS 2, navedeni v Prilogi I k Uredbi (ES) št. 1059/2003	– subjekti javne uprave regij na ravni NUTS 2, navedeni v Prilogi I k Uredbi (ES) št. 1059/2003 ([***27 b (novo)***])
[27] Uredba (ES) št. 1059/2003 Evropskega parlamenta in Sveta z dne 26. maja 2003 o oblikovanju skupne klasifikacije statističnih teritorialnih enot (nuts) (UL L 154, 21.6.2003, str. 1).	[27] Uredba (ES) št. 1059/2003 Evropskega parlamenta in Sveta z dne 26. maja 2003 o oblikovanju skupne klasifikacije statističnih teritorialnih enot (nuts) (UL L 154, 21.6.2003, str. 1). ***[27 a (novo)] Ali enakovredne upravne enote v državah članicah, v katerih se klasifikacija NUTS še ni vključena v institucionalno upravno ureditev.*** ***[27 b (novo)] Ali enakovredne upravne enote v državah članicah, v katerih se klasifikacija NUTS še ni vključena v institucionalno upravno ureditev.***

POSTOPEK V ODBORU, ZAPROŠENEM ZA MNENJE

Naslov	Ukrepi za visoko skupno raven kibernetske varnosti v Uniji in razveljavitev Direktive (EU) 2016/1148
Referenčni dokumenti	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Pristojni odbor Datum razglasitve na zasedanju	ITRE 21.1.2021
Mnenje pripravil Datum razglasitve na zasedanju	AFET 21.1.2021
Pripravljavec/-ka mnenja Datum imenovanja	Markéta Gregorová 22.2.2021
Obravnava v odboru	25.5.2021 16.6.2021 17.6.2021
Datum sprejetja	14.7.2021
Izid končnega glasovanja	+: 59 –: 5 0: 6
Poslanci, navzoči pri končnem glasovanju	Alviina Alametsä, Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Jorgos Jeorjiu (Giorgos Georgiou), Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk (Ilhan Kyuchyuk), David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Dimitris Papadakis (Demetris Papadakis), Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergej Stanišev (Sergei Stanishev), Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Namestniki, navzoči pri končnem glasovanju	Ioan-Rareş Bogdan, Andrej Kovačev (Andrey Kovatchev), Marisa Matias, Gabriel Mato, Milan Zver

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V ODBORU, ZAPROŠENEM ZA MNENJE

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Aleksander Aleksandrov Jordanov (Alexander Alexandrov Yordanov), Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrej Kovačev (Andrey Kovatchev), Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
Renew	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk (Ilhan Kyuchyuk), Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Dimitris Papadakis (Demetris Papadakis), Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergej Stanišev (Sergei Stanishev)
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Jorgos Jeorjiu (Giorgos Georgiou), Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

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