EVROPSKA
KOMISIJA

Bruselj, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji

{SWD(2013) 31 final}
{SWD(2013) 32 final}

OBRAZLOŽITVENI MEMORANDUM

Predlagana direktiva naj bi zagotovila visoko skupno raven varnosti omrežij in informacij (v nadaljnjem besedilu: VOI). V ospredju je izboljšanje varnosti interneta ter zasebnih omrežij in informacijskih sistemov, ki podpirajo delovanje naše družbe in gospodarstva. To bo doseženo tako, da se bosta od držav članic zahtevala večja pripravljenost in boljše medsebojno sodelovanje, od javnih uprav in upravljavcev kritičnih infrastruktur, kot so energija in promet, ter ključnih ponudnikov storitev informacijske družbe (platforme za e-trgovanje, družabna omrežja itd.) pa, da sprejmejo ustrezne ukrepe za obvladovanje varnostnih tveganj in resne incidente priglasijo nacionalnim pristojnim organom.

Ta predlog se navezuje na skupno sporočilo Komisije in visokega predstavnika Unije za zunanje zadeve in varnostno politiko o evropski strategiji za kibernetsko varnost. Cilj strategije je zagotoviti varno in zaupanja vredno digitalno okolje ter hkrati spodbujati in varovati temeljne pravice in druge osrednje vrednote EU. Ta predlog je glavni ukrep strategije. Nadaljnji ukrepi strategije na tem področju so usmerjeni v ozaveščanje, razvoj notranjega trga kibernetskih izdelkov in storitev ter spodbujanje naložb v raziskave in razvoj. Dopolnjevali jih bodo tudi drugi ukrepi za okrepljen boj proti kibernetski kriminaliteti in oblikovanje mednarodne politike kibernetske varnosti za EU.

1.1. Razlogi za predlog in njegovi cilji

VOI je vse bolj pomembna za evropsko gospodarstvo in družbo. Je pomemben pogoj za vzpostavitev zanesljivega okolja za svetovno trgovino s storitvami. Informacijske sisteme lahko ogrozijo varnostni incidenti, ki so lahko posledica človeških napak, naravnih dogodkov, tehničnih okvar ali zlonamernih napadov. Ti incidenti so vse obsežnejši, pogostejši in bolj zapleteni. Komisija je v javnem spletnem posvetovanju o izboljšanju VOI v EU[1] ugotovila, da je bilo 57 % vprašanih prejšnje leto priča incidentom VOI z resnimi posledicami za njihove dejavnosti. Pomanjkanje VOI lahko ogrozi ključne storitve, ki so odvisne od celovitosti omrežij in informacijskih sistemov. To lahko ustavi delovanje podjetij, ustvari znatne finančne izgube za gospodarstvo EU in negativno vpliva na družbeno dobro.

Poleg tega so digitalni informacijski sistemi, zlasti internet, čezmejni komunikacijski instrument; to pomeni, da so med seboj povezani po vseh državah članicah in da imajo ključno vlogo pri čezmejnem pretoku blaga, storitev in oseb. Znatne motnje teh sistemov v eni državi članici lahko vplivajo na druge države članice in na EU kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za dokončno vzpostavitev enotnega digitalnega trga in nemoteno delovanje notranjega trga. Verjetnost in pogostost incidentov ter nezmožnost zagotavljanja učinkovite zaščite prav tako zmanjšujejo zaupanje javnosti v omrežja in informacijske storitve. Leta 2012 je raziskava Eurobarometra o kibernetski varnosti na primer pokazala, da ima 38 % uporabnikov interneta v EU pomisleke o varnosti spletnih plačil, zaradi česar so spremenili svoje vedenje: 18 % jih je manj naklonjenih spletnemu nakupovanju, 15 % pa manj naklonjenih uporabi spletnega bančništva[2].

Trenutne razmere, ki so rezultat zgolj prostovoljnega ukrepanja, v EU ne zagotavljajo zadostne zaščite pred incidenti in tveganji VOI. Obstoječe zmogljivosti in mehanizmi VOI preprosto ne zadoščajo za dohajanje hitro spreminjajočih se nevarnosti in zagotavljanje skupne visoke ravni zaščite v vseh državah članicah.

---

[1] Javno spletno posvetovanje o „izboljšanju varnosti omrežij in informacij v EU“ je potekalo od 23. julija do 15. oktobra 2012.

[2] Eurobarometer 390/2012.

Kljub sprejetim pobudam se zmogljivosti in pripravljenost v državah članicah zelo različne, zaradi česar so tudi pristopi v EU razdrobljeni. Omrežja in informacijski sistemi so med seboj povezani, zato skupno VOI slabijo države članice z nezadostno zaščito. Ta prav tako ovira vzpostavitev zaupanja med partnerji, kar je pogoj za sodelovanje in izmenjavo informacij. Zato je sodelovanje vzpostavljeno le med nekaj državami članicami z visoko ravnijo zmogljivosti.

Zaradi tega trenutno na ravni EU ni učinkovitega mehanizma za učinkovito sodelovanje in zanesljivo izmenjavo informacij o incidentih in tveganjih VOI med državami članicami. To lahko privede do neusklajenih regulativnih posegov, neskladnih strategij in različnih standardov ter s tem do nezadostne zaščite pred incidenti VOI po vsej EU. Na notranjem trgu se lahko pojavijo tudi ovire, ki bi za podjetja, ki poslujejo v več kot eni državi članici, pomenile stroške usklajevanja.

Poleg tega za akterje, ki upravljajo kritično infrastrukturo ali zagotavljajo storitve, bistvene za delovanje naše družbe, ne veljajo ustrezne obveznosti za sprejetje ukrepov za obvladovanje tveganja in izmenjavo informacij z zadevnimi organi. Na eni strani zato podjetja nimajo učinkovitih spodbud za resno obvladovanje tveganja, ki bi vključevalo oceno tveganja in ustrezne ukrepe za zagotovitev VOI. Po drugi strani pa pristojni organi o velikem deležu incidentov sploh niso obveščeni in jih zato ne opazijo. Obveščanje o incidentih je bistvenega pomena, saj se le tako javni organi lahko nanje odzovejo, sprejmejo ustrezne ukrepe za zmanjšanje tveganja in določijo strateške prednostne naloge za VOI.

Veljavni regulativni okvir sprejetje ukrepov za obvladovanje tveganja in priglasitev resnih incidentov VOI nalaga samo telekomunikacijskim družbam. Vendar so tudi številni drugi sektorji odvisni od IKT kot omogočitvenih tehnologij in bi zato prav tako morali obravnavati vprašanje VOI. Nekateri ponudniki infrastrukture in storitev so še posebej ranljivi, saj so zelo odvisni od pravilnega delovanja omrežij in informacijskih sistemov. Ti sektorji imajo pomembno vlogo pri zagotavljanju ključnih podpornih storitev za naše gospodarstvo in družbo, varnost njihovih sistemov pa je zlasti pomembna za delovanje notranjega trga. To so med drugim bančništvo, borze, proizvodnja, prenos in distribucija energije, promet (zračni, železniški, pomorski), zdravje, internetne storitve in javne uprave.

Zato je treba VOI v EU začeti obravnavati drugače. Potrebne so regulativne obveznosti, ki bodo zagotovile enake konkurenčne pogoje in odpravile obstoječe zakonodajne vrzeli. Za zagotovitev enakih konkurenčnih pogojev in odpravo obstoječih zakonodajnih vrzeli so potrebne regulativne obveznosti. Za odpravljanje teh težav in povečanje ravni VOI v EU predlagana direktiva določa naslednje cilje:

prvič, v skladu s predlogom naj bi vse države članice zagotovile minimalno raven nacionalnih zmogljivosti tako, da imenujejo organe, pristojne za VOI, ustanovijo skupine za odzivanje na računalniške grožnje ter sprejmejo nacionalne strategije VOI in nacionalne načrte sodelovanja na področju VOI;

drugič, pristojni nacionalni organi bi morali sodelovati v mreži, prek katere bi se omogočilo varno in učinkovito usklajevanje, kar med drugim vključuje usklajeno izmenjavo informacij ter odkrivanje in odzivanje na ravni EU. V tej mreži bi si države članice morale izmenjevati informacije ter sodelovati pri obvladovanju groženj in incidentov VOI na podlagi evropskega načrta sodelovanja na področju VOI;

tretjič, na podlagi modela okvirne direktive o elektronskih komunikacijah naj bi predlog zagotovil, da se razvije kultura obvladovanja tveganja ter izmenjujejo informacije med zasebnim in javnim sektorjem. Javne uprave in podjetja v nekaterih navedenih kritičnih sektorjih bodo morali oceniti tveganja, s katerimi se soočajo, ter sprejeti ustrezne in

sorazmerne ukrepe za zagotovitev VOI. Ti subjekti bodo morali pristojnim organom poročati o vseh incidentih, ki resno ogrožajo njihova omrežja in informacijske sisteme ter znatno vplivajo na neprekinjenost kritičnih storitev in dobavo blaga.

1.2. Splošno ozadje

Komisija je že leta 2001 v sporočilu „Varnost omrežij in informacij: predlog za evropski politični pristop“ izpostavila vse večji pomen VOI[3]. Nato je leta 2006 sprejela strategijo za varno informacijsko družbo[4], katere namen je bil v Evropi razviti kulturo VOI. Glavne elemente strategije je Svet potrdil z resolucijo[5].

Komisija je 30. marca 2009 sprejela tudi sporočilo o zaščiti kritične informacijske infrastrukture[6], v katerem je poudarila, da je treba Evropo zaščititi pred kibernetskimi prekinitvami s povečanjem varnosti. S tem sporočilom se je začel izvajati akcijski načrt, ki je podprl prizadevanja držav članic, da zagotovijo preprečevanje in odzivanje. Akcijski načrt je v svojih sklepih potrdilo predsedstvo ministrske konference o zaščiti kritične informacijske infrastrukture v Talinu leta 2009. Svet je 18. decembra 2009 sprejel resolucijo o „skupnem evropskem pristopu do varnosti omrežij in informacij “[7].

V Evropski digitalni agendi[8], sprejeti maja 2010, in z njo povezanih sklepih Sveta[9] je izpostavljeno soglasje, da sta zaupanje in varnost temeljna pogoja za široko uporabo IKT in s tem doseganje ciljev „pametne rasti“ v okviru strategije Evropa 2020[10]. V Evropski digitalni agendi je v poglavju „Zaupanje in varnost“ poudarjeno, da se morajo vse zainteresirane strani z združenimi močmi celovito prizadevati za varnost in odpornost infrastrukture IKT, pri čemer se morajo osredotočiti na preprečevanje, pripravljenost in ozaveščanje ter razviti usklajene varnostne mehanizme. Evropska digitalna agenda zlasti z ukrepom št. 6 poziva k ukrepom, ki naj bi okrepili politiko VOI na visoki ravni.

V sporočilu o zaščiti kritične informacijske infrastrukture iz marca 2011 „Dosežki in naslednji koraki: h globalni kibernetski varnosti“[11] je Komisija ocenila dosežke od sprejetja akcijskega načrta za zaščito kritične informacijske infrastrukture iz leta 2009 in ugotovila, da je izvajanje načrta pokazalo, da izključno nacionalni pristopi za reševanje izzivov na področju varnosti in odpornosti niso dovolj in da si mora Evropa še naprej prizadevati za skladen in na sodelovanju temelječ pristop na ravni EU. V sporočilu o zaščiti kritične informacijske infrastrukture iz leta 2011 je Komisija napovedala več ukrepov ter države članice pozvala, naj okrepijo zmogljivosti VOI in čezmejno sodelovanje. Večina teh ukrepov bi morala biti zaključena do leta 2012, vendar do zdaj še niso bili izvedeni.

V sklepih z dne 27. maja 2011 o zaščiti kritične informacijske infrastrukture je Svet Evropske unije poudaril, da morajo biti sistemi IKT in omrežja odporni in varni pred vsemi morebitnimi prekinitvami, tako naključnimi kot namernimi, da je treba v EU doseči visoko raven pripravljenosti, varnosti in odpornosti, izboljšati strokovno usposobljenost, da se bo Evropa lahko soočila z izzivi zaščite omrežij in informacijske infrastrukture, ter spodbujati

---

3 COM(2001) 298.

4 COM(2006) 251, https://webgate.ec.testa.eu/docfinder/extern/aHR0cDovLw==/ZXVyLWxleC5ldXJvcGEuZXU=/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:SL:PDF.

5 2007/068/01.

6 COM(2009) 149.

7 2009/C 321/01.

8 COM(2010) 245.

9 Sklepi Sveta z dne 31. maja 2010 o evropski digitalni agendi (10130/10).

10 COM(2010) 2020 in sklepi Evropskega sveta z dne 25. in 26. marca 2010 (EUCO 7/10).

11 COM(2011) 163.

vzpostavitev mehanizmov za sodelovanje pri kibernetskih incidentih med državami članicami ter tako izboljšati sodelovanje med njimi.

1.3. Veljavne evropske in mednarodne določbe na tem področju

Z Uredbo (ES) št. 460/2004 je Evropska skupnost leta 2004 ustanovila Evropsko agencijo za varnost omrežij in informacij (ENISA)[12], ki naj bi prispevala k zagotavljanju visoke ravni VOI in razvoju kulture VOI v EU. Predlog za posodobitev mandata ENISA je bil sprejet 30. septembra 2010[13] ter ga trenutno obravnavata Svet in Evropski parlament. Revidirani regulativni okvir za elektronske komunikacije[14], ki velja od novembra 2009, ponudnikom elektronskih komunikacij nalaga varnostne obveznosti[15]. Te obveznosti je bilo treba na nacionalni ravni prenesti do maja 2011.

Vse akterje, ki so upravljavci podatkov (na primer banke ali bolnišnice), zakonodajni okvir EU za varstvo podatkov[16] obvezuje, da sprejmejo varnostne ukrepe za varstvo osebnih podatkov. Prav tako morajo po Komisijinem predlogu uredbe o splošnem varstvu podatkov iz leta 2012[17] upravljavci podatkov nacionalnim nadzornim organom poročati o kršitvah varstva osebnih podatkov. To na primer pomeni, da kršitve VOI, ki vpliva na zagotavljanje storitve, vendar ne ogroža varstva osebnih podatkov (npr. izpad IKT v energetski družbi, ki povzroči popoln izpad električne energije), ne bi bilo treba priglasiti.

V okviru Direktive 2008/114 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite „Evropski program za varovanje ključne infrastrukture (EPCIP)“[18] določa splošni „krovni“ pristop za zaščito kritične infrastrukture v EU. Cilji EPCIP so v celoti v skladu s tem predlogom, ta direktiva pa bi se morala uporabljati ne glede na Direktivo 2008/114. EPCIP izvajalcev ne obvezuje, da poročajo o pomembnih kršitvah varnosti, niti ne določa mehanizmov za države članice, prek katerih bi te lahko sodelovale in se odzivale na incidente.

Sozakonodajalca zdaj razpravljata o Komisijinem predlogu direktive o napadih na informacijske sisteme[19], s katero naj bi se harmonizirala kriminalizacija določenih vrst ravnanja. Direktiva ureja samo kriminalizacijo nekaterih vrst ravnanja ter ne obravnava preprečevanja tveganj in incidentov VOI, odzivanja na incidente VOI in ublažitev njihovih učinkov. Ta direktiva bi se morala uporabljati ne glede na direktivo o napadih na informacijske sisteme.

Komisija je 28. marca 2012 sprejela sporočilo o ustanovitvi Evropskega centra za boj proti kibernetski kriminaliteti[20]. Center, ustanovljen 11. januarja 2013, je del Evropskega policijskega urada (Europola) in bo deloval kot osrednja točka v boju proti kibernetski kriminaliteti v EU. Njegov namen je združiti evropsko strokovno znanje o kibernetski kriminaliteti in podpreti države članice pri gradnji zmogljivosti in preiskovanju kibernetske

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:SL:HTML.

13 COM(2010) 521.

14 Glej http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Člena 13a in 13b okvirne direktive.

16 Direktiva 2002/58 z dne 12. julija 2002.

17 COM(2012) 11.

18 COM(2006) 786, https://webgate.ec.testa.eu/docfinder/extern/aHR0cDovLw==/ZXVyLWxleC5ldXJvcGEuZXU=/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:SL:PDF.

19 COM(2010) 517 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:SL:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:SL:PDF.

kriminalitete, ob tem pa v tesnem sodelovanju z Eurojustom postati skupni glas vseh evropskih organov kazenskega pregona in sodstva, ki preiskujejo kibernetsko kriminaliteto.

Evropske institucije, agencije in organi so ustanovili lastne skupine za odzivanje na računalniške grožnje (CERT).

Na mednarodni ravni je EU dejavna na področju kibernetske varnosti na dvostranski in večstranski ravni. Na vrhu EU–ZDA leta 2010[21] je bila ustanovljena delovna skupina EU–ZDA za kibernetsko varnost in kibernetsko kriminaliteto. EU je dejavna tudi v drugih pomembnih večstranskih forumih, na primer Organizaciji za gospodarsko sodelovanje in razvoj (OECD), Generalni skupščini Združenih narodov (GS ZN), Mednarodni telekomunikacijski zvezi (ITU), Organizaciji za varnost in sodelovanje v Evropi (OVCE), Svetovnem vrhu o informacijski družbi (WSIS) in Forumu za upravljanje interneta (IGF).

2. REZULTATI POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

2.1. Posvetovanja z zainteresiranimi stranmi in uporaba izvedenskih mnenj

Javno spletno posvetovanje o „izboljšanju VOI v EU“ je potekalo med 23. julijem in 15. oktobrom 2012. Komisija je na spletni vprašalnik prejela skupaj 160 odgovorov.

Ključne ugotovitve so bile, da zainteresirane strani na splošno podpirajo izboljšanje VOI po vsej EU. Podrobneje: 82,8 % vprašanih je menilo, da bi vlade v EU morale storiti več za zagotovitev visoke ravni VOI; 82,8 % jih je menilo, da se uporabniki informacij in sistemov ne zavedajo obstoječih groženj in incidentov VOI; načeloma bi jih 66,3 % podprlo uvedbo regulativne zahteve za obvladovanje tveganj VOI; 84,8 % pa jih je izjavilo, da bi bilo treba takšne zahteve določiti na ravni EU. Veliko vprašanih je menilo, da bi bilo pomembno, da se sprejmejo zahteve VOI zlasti v naslednjih sektorjih: bančništvo in finance (91,1 %), energija (89,4 %), promet (81,7 %), zdravje (89,4 %), internetne storitve (89,1 %) in javne uprave (87,5 %). Poleg tega so vprašani menili, da bi morala biti morebitna zahteva za poročanje o kršitvah VOI nacionalnim pristojnim organom določena na ravni EU (65,1%), in potrdili, da bi morala veljati tudi za javne uprave (93,5 %). Poleg tega so poudarili, da zahteva za izvajanje ukrepov za obvladovanje tveganja VOI glede na trenutno stanje za njih ne bi pomenila znatnih dodatnih stroškov (63,4 %), enako velja za zahtevo o poročanju o kršitvah varnosti (72,3 %).

Posvetovanja z državami članicami so bila opravljena v okviru več pristojnih sestav Sveta, v okviru Evropskega foruma za države članice na konferenci o kibernetski varnosti, ki sta jo organizirali Komisija in Evropska služba za zunanje delovanje 6. julija 2012, ter na posebnih dvostranskih srečanjih, sklicanih na zahtevo posameznih držav članic.

Razprave z zasebnim sektorjem so bile organizirane v okviru evropskega javno-zasebnega partnerstva za odpornost[22] in na dvostranskih srečanjih. Za institucije EU je Komisija organizirala razprave z ENISA in CERT.

2.2. Ocena učinka

Komisija je opravila oceno učinka za tri možnosti politike:

Možnost 1: brez sprememb (izhodiščni scenarij) – ohranitev obstoječega pristopa;

---

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

22 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

Možnost 2: regulativni pristop, sestavljen iz zakonodajnega predloga za vzpostavitev skupnega pravnega okvira EU za VOI za zmogljivosti držav članic, mehanizme za sodelovanje na ravni EU ter zahteve za ključne zasebne akterje in javne uprave;

Možnost 3: mešani pristop, ki združuje prostovoljne pobude za zmogljivosti VOI držav članic in mehanizme za sodelovanje na ravni EU z regulativnimi zahtevami za ključne zasebne akterje in javne uprave.

Komisija je ugotovila, da bi imela možnost 2 največje pozitivne učinke, saj bi se z njo znatno izboljšalo varstvo potrošnikov, podjetij in uprav EU pred incidenti VOI. Zlasti bi obveznosti za države članice zagotovile ustrezno pripravljenost na nacionalni ravni ter prispevale k medsebojnem zaupanju, ki je pogoj za učinkovito sodelovanje na ravni EU. Mehanizmi za sodelovanje na ravni EU prek mreže bi zagotovili dosledno in usklajeno preprečevanje in odzivanje na čezmejne incidente in tveganja VOI. Uvedba zahtev za izvajanje ukrepov za obvladovanje tveganj VOI za javne uprave in ključne zasebne akterje bi pomenila močno spodbudo za učinkovito obvladovanje varnostnih tveganj. Obveznost o poročanju o incidentih VOI z znatnim vplivom bi izboljšala sposobnost odzivanja na incidente in spodbujala preglednost. Poleg tega bi EU pometla pred svojim pragom in razširila svoj mednarodni vpliv ter postala še bolj verodostojen partner za sodelovanje na dvostranski in večstranski ravni. EU bi bila tudi v boljšem položaju za spodbujanje temeljnih pravic in vrednot EU v tujini.

Kvantitativna ocena je pokazala, da možnost 2 za države članice ne bi pomenila nesorazmerne obremenitve. Stroški za zasebni sektor prav tako ne bi bili visoki, saj naj bi številni zadevni subjekti že zdaj izpolnjevali obstoječe varnostne zahteve (tj. obveznost za upravljavce podatkov, da sprejmejo tehnične in organizacijske ukrepe za varstvo osebnih podatkov, vključno z ukrepi na področju VOI). Upoštevani so bili tudi obstoječi izdatki za varnost v zasebnem sektorju.

Ta predlog upošteva načela Listine Evropske unije o temeljnih pravicah, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo podjetniške pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva pred sodiščem in pravico vsake osebe do izjave. To direktivo je treba izvajati v skladu s temi pravicami in načeli.

3. PRAVNI ELEMENTI PREDLOGA

3.1. Pravna podlaga

Evropska unija je pooblaščena, da sprejme ukrepe za vzpostavitev ali zagotavljanje delovanja notranjega trga v skladu z ustreznimi določbami pogodb (člen 26 Pogodbe o delovanju Evropske unije – PDEU). V skladu s členom 114 PDEU lahko EU sprejme „ukrepe za približevanje določb zakonov in drugih predpisov v državah članicah, katerih predmet je vzpostavitev in delovanje notranjega trga“.

Kot je navedeno zgoraj, imajo omrežja in informacijski sistemi ključno vlogo pri čezmejnem pretoku blaga, storitev in oseb. Pogosto so med seboj povezani, internet pa ima globalni značaj. Zaradi čeznacionalne razsežnosti lahko prekinitev v eni državi članici vpliva tudi na druge države članice in na EU kot celoto. Odpornost in stabilnost omrežij in informacijskih sistemov je zato bistvenega pomena za nemoteno delovanje notranjega trga.

Zakonodajalec EU je že potrdil potrebo po harmonizaciji pravil na področju VOI, da bi zagotovil razvoj notranjega trga. To zlasti velja za Uredbo št. 460/2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij[23], ki temelji na členu 114 PDEU.

Razlike, nastale zaradi neenakih nacionalnih zmogljivostih VOI, politikah in ravneh zaščite v državah članicah, ovirajo notranji trg in upravičujejo ukrepanje na ravni EU.

3.2. Subsidiarnost

Evropsko ukrepanje na področju VOI upravičuje načelo subsidiarnosti.

Prvič, glede na čezmejno naravo VOI bi neukrepanje na ravni EU povzročilo, da bi vsaka država članica ukrepala sama, pri tem pa se ne bi upoštevale soodvisnosti med omrežji in informacijskimi sistemi EU. Ustrezna stopnja usklajenosti med državami članicami bi zagotovila dobro obvladovanje tveganj VOI v čezmejnem okviru, v katerem se pojavljajo. Razlike v predpisih s področja VOI ovirajo podjetja, ki želijo poslovati v več državah, in svetovne ekonomije obsega.

Drugič, regulativne obveznosti na ravni EU so potrebne, da se ustvarijo enaki konkurenčni pogoji in odpravijo zakonodajne vrzeli. Povsem prostovoljni pristop je vzpostavil sodelovanje samo med manjšino držav članic, ki že imajo visoko raven zmogljivosti. Da bi bile vključene vse države članice, je treba zagotoviti, da bodo vse dosegale minimalno raven zmogljivosti. Ukrepi VOI, ki jih sprejmejo vlade, morajo biti med seboj skladni in usklajeni ter obravnavati in zmanjševati posledice incidentov VOI. V mreži si bodo ENISA, pristojni organi in Komisija izmenjevali najboljše prakse in stalno sodelovali, da bi omogočili usklajeno izvajanje direktive po vsej EU. Poleg tega lahko usklajeni politični ukrepi na področju VOI bistveno prispevajo k učinkoviti zaščiti temeljnih pravic, zlasti pravice do varstva osebnih podatkov in zasebnosti. Ukrepanje na ravni EU bi tako izboljšalo učinkovitost obstoječih nacionalnih politik in olajšalo njihov razvoj.

Predlagani ukrepi so upravičeni tudi z vidika sorazmernosti. Državam članicam so naložene najmanjše možne zahteve, ki še zagotavljajo ustrezno pripravljenost in vzpostavitev na zaupanju temelječega sodelovanja. Tako lahko države članice upoštevajo tudi nacionalne posebnosti, ob tem pa se skupna načela EU uporabljajo sorazmerno. Široko področje uporabe bo državam članicam omogočilo, da direktivo izvajajo glede na dejanska tveganja na nacionalni ravni v skladu z nacionalno strategijo VOI. Zahteve za obvladovanje tveganja se nanašajo samo na kritične subjekte in nalagajo ukrepe, ki so sorazmerni s tveganji. Na javnem posvetovanju je bil poudarjen pomen zagotavljanja varnosti teh kritičnih subjektov. Zahteve poročanja bi se nanašale samo na incidente z znatnim učinkom. Kot je navedeno zgoraj, ukrepi ne bi nalagali nesorazmernih stroškov, saj mnoge od teh subjektov kot upravljavce podatkov pravila za varstvo podatkov že sedaj obvezujejo, da zagotovijo varstvo osebnih podatkov.

Da ne bi bili mali operaterji, zlasti MSP, nesorazmerno obremenjeni, bi morale biti zahteve sorazmerne s tveganjem, ki mu je izpostavljeno zadevno omrežje ali informacijski sistem, in ne bi smele veljati za mikropodjetja. Opredelitev tveganja je v prvi vrsti naloga subjektov, za katere veljajo te zahteve, zato morajo ti subjekti določiti tudi ukrepe za ublažitev tveganj.

Navedene cilje je zaradi čezmejnih vidikov incidentov in tveganj VOI lažje doseči na ravni EU kot na ravni posameznih držav članic. Unija lahko zato sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom

[23] Uredba (ES) št. 460/2004 Evropskega Parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij (UL L 077, 13.3.2004, str. 1).

sorazmernosti predlagana uredba ne presega tega, kar je potrebno za uresničitev navedenih ciljev.

Da bi Komisija dosegla cilje, bi morala biti pooblaščena za sprejemanje delegiranih aktov v skladu s členom 290 Pogodbe o delovanju Evropske unije, da bi lahko dopolnila ali spremenila nekatere nebistvene elemente osnovnega akta. Komisijin predlog spodbuja tudi sorazmerno izvajanje zahtev, ki so naložene zasebnim in javnim udeležencem.

Da se zagotovijo enotni pogoji za izvajanje temeljnega akta, bi bilo treba Komisijo pooblastiti za sprejemanje izvedbenih aktov v skladu s členom 291 PDEU.

Zaradi širokega obsega uporabe predlagane direktive, zaradi dejstva, da ureja močno regulirana področja, in zaradi pravnih obveznosti iz poglavja IV, bi morali obvestilo o ukrepih prenosa spremljati obrazložitveni dokumenti. 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.

4. PRORAČUNSKE POSLEDICE

Sodelovanje in izmenjavo informacij med državami članicami bi morala podpirati varna infrastruktura. Predlog bo imel proračunske posledice le, če se države članice odločijo prilagoditi obstoječo infrastrukturo (npr. sTESTA) in Komisiji naložijo, da prilagoditev opravi v okviru večletnega finančnega okvira za obdobje 2014–2020. Enkratni stroški so ocenjeni na 1 250 000 EUR in bi se krili iz proračuna EU, proračunska vrstica 09.03.02 (za spodbujanje medsebojnega povezovanja in interoperabilnosti nacionalnih javnih storitev na spletu ter dostop do takih omrežij – poglavje 09.03, instrument za povezovanje Evrope – telekomunikacijska omrežja), pod pogojem, da je v okviru IPE na voljo dovolj sredstev. Druga možnost je, da si države članice delijo enkratne stroške prilagoditve obstoječe infrastrukture oziroma se odločijo, da bodo vzpostavile novo infrastrukturo ter krile stroške, ki so ocenjeni na približno 10 milijonov EUR letno.

2013/0027 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije, zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po predložitvi osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[1],

po posvetovanju z Evropskim nadzornikom za varstvo podatkov,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(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.

(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.

(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.

(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.

(5) Da bi ta direktiva obravnavala vse pomembne incidente in tveganja, bi morala veljati za vsa omrežja in informacijske sisteme. Vendar obveznosti za javne uprave in tržne udeležence ne bi smele veljati za podjetja, ki zagotavljajo javna komunikacijska

[1] UL C […], […], str. […].

omrežja ali javno dostopne elektronske komunikacijske storitve po Direktivi 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva)[2] in za katera veljajo posebne zahteve glede varnosti in celovitosti iz člena 13a navedene direktive, kot tudi ne za ponudnike skrbniških storitev.

(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.

(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.

(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.

(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.

(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.

(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.

(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.

[2] UL L 108, 24.4.2002, str. 33.

(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.

(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.

(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.

(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.

(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.

(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.

(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.

(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.

(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.

(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.

(23) Direktiva 2002/21/ES določa, da podjetja, ki zagotavljajo javna elektronska komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve, sprejmejo ustrezne ukrepe, s katerimi zagotovijo celovitost in varnost teh omrežij in sistemov, uvaja pa tudi zahteve za priglasitev kršitev varnosti in izgube integritete. Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah)[3] določa, da ponudnik javno razpoložljive elektronske komunikacijske storitve sprejme ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi varnost svojih storitev.

(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[4], 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 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.

(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.

(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.

(27) Da ne bi bili mali operaterji in uporabniki nesorazmerno finančno in upravno obremenjeni, bi morale biti zahteve sorazmerne s tveganjem, ki mu je izpostavljeno zadevno omrežje ali informacijski sistem, pri čemer bi bilo treba upoštevati trenutno stanje takih ukrepov. Te zahteve se ne bi smele uporabljati za mikropodjetja.

---

[3] UL L 201, 31.7.2002, str. 37.
[4] UL L 204, 21.7.1998, str. 37.

(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.

(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.

(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.

(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[5], 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.

(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[6].

(33) Komisija bi morala redno pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim tehnološkim in tržnim razmeram.

---

5 SEC(2012) 72 final.

6 UL L 316, 14.11.2012, str. 12.

(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.

(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.

(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[7].

(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.

(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.

(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[8]. 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.

(40) Ker ciljev te direktive, in sicer zagotavljanja visoke ravni VOI v Uniji, države članice same ne morejo zadovoljivo doseči in ker se ta cilj zaradi učinkov ukrepov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti

[7] UL L 55, 28.2.2011, str. 13.
[8] UL L 145, 31.5.2001, str. 43.

iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta direktiva ne presega tistega, kar je potrebno, da se dosežejo navedeni cilji.

(41) Ta direktiva upošteva temeljne pravice in načela Listine Evropske unije o temeljnih pravicah, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo podjetniške pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča in pravico vsake osebe do izjave. To direktivo je treba izvajati v skladu s temi pravicami in načeli.

SPREJELA NASLEDNJO DIREKTIVO:

POGLAVJE I
SPLOŠNE DOLOČBE

Člen 1

Vsebina in področje uporabe

1. Ta direktiva določa ukrepe za zagotavljanje visoke skupne ravni varnosti omrežij in informacij (v nadaljnjem besedilu: VOI) v Uniji.

2. V ta namen ta direktiva:

(a) določa obveznosti za vse države članice glede preprečevanja, obravnavanja in odzivanja 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;

(c) določa varnostne zahteve za tržne udeležence in javne uprave.

3. Varnostne zahteve iz člena 14 se ne uporabljajo za podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve v skladu z Direktivo 2002/21/ES in za katera veljajo posebne zahteve glede varnosti in celovitosti iz člena 13a in 13b navedene direktive, kot tudi ne za ponudnike skrbniških storitev.

4. Ta direktiva ne posega v zakonodajo EU o kibernetski kriminaliteti ter Direktivo Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite[9].

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[10], 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[11].

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

[9] UL L 345, 23.12.2008, str. 75.
[10] UL L 281, 23.11.1995, str. 31.
[11] SEC(2012) 72 final.

si prizadeva ta direktiva, in jo države članice odobrijo v skladu s členom 7 Direktive 95/46/ES in Direktivo 2002/58/ES, kakor se izvajata v nacionalni zakonodaji.

Člen 2

Minimalna harmonizacija

Ne glede na obveznosti po zakonodaji Unije se državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo stopnjo varnosti.

Člen 3

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

(1) „omrežje in informacijski sistem“ pomeni:

(a) elektronsko komunikacijsko omrežje po Direktivi 2002/21/ES in

(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

(c) računalniške podatke, ki jih elementi iz točke (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

(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,

(3) „tveganje“ pomeni vsako okoliščino ali dogodek, ki ima lahko negativen učinek na varnost;

(4) „incident“ pomeni vsako okoliščino ali dogodek, ki ima dejanski negativen učinek na varnost;

(5) „storitev informacijske družbe“ pomeni storitev po točki (2) člena 1 Direktive 98/34/ES;

(6) „načrt za sodelovanje na področju VOI“ pomeni načrt za vzpostavitev okvira za organizacijske naloge, pristojnosti in postopke za ohranjanje ali ponovno vzpostavitev delovanja omrežij in informacijskih sistemov, če jih prizadene tveganje ali incident;

(7) „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo analizo, ublažitev in odzivanje na incidente;

(8) „tržni udeleženec“ pomeni:

(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;

(9) „standard“ pomeni standard iz Uredbe (EU) št. 1025/2012;

(10) „specifikacija“ pomeni specifikacijo iz Uredbe (EU) št. 1025/2012;

(11) „ponudnik skrbniških storitev“ pomeni fizično ali pravno osebo, ki zagotavlja elektronsko storitev, ki vključuje ustvarjanje, preverjanje, potrjevanje, obdelavo in hrambo elektronskih podpisov, elektronskih žigov, elektronskih časovnih žigov, elektronskih dokumentov, storitev elektronske dostave, avtentikacije spletišč in elektronskih certifikatov, vključno s certifikati za elektronski podpis in elektronske žige.

POGLAVJE II

NACIONALNI OKVIRI ZA VARNOST OMREŽIJ IN INFORMACIJ

Člen 4

Načelo

Države članice v skladu s to direktivo zagotavljajo visoko raven varnosti omrežij in informacijskih sistemov na svojem ozemlju.

Člen 5

Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI

1. Vsaka država članica sprejme nacionalno strategijo VOI, v kateri določi strateške cilje in konkretne ukrepe, s katerimi bo dosegla in vzdrževala visoko raven VOI.NV nacionalni strategiji VOI so obravnavani zlasti:

(a) opredelitev ciljev in prednostnih nalog strategije na podlagi posodobljene analize tveganja in incidentov;

(b) okvir upravljanja za dosego ciljev in prednostnih nalog strategije, ki vključuje jasno opredelitev vloge in odgovornosti vladnih organov in drugih ustreznih akterjev;

(c) opredelitev splošnih ukrepov za pripravljenost, odzivanje in ponovno vzpostavitev, vključno z mehanizmi za sodelovanje med javnim in zasebnim sektorjem;

(d) določitev programov izobraževanja, ozaveščanja in usposabljanja;

(e) načrte za raziskave in razvoj ter opis, kako ti načrti ustrezajo opredeljenim prednostnim nalogam.

2. Nacionalna strategija VOI vključuje nacionalni načrt za sodelovanje na področju VOI, ki vsebuje najmanj naslednje:

(a) načrt ocene tveganja za prepoznavanje tveganj in ocenjevanje učinkov morebitnih incidentov;

(b) opredelitev vloge in odgovornosti različnih akterjev, vključenih v izvajanje načrta;

(c) opredelitev postopkov sodelovanja in komuniciranja za preprečevanje, odkrivanje, odzivanje, popravilo in ponovno vzpostavitev, ki so oblikovani glede na opozorilno stopnjo;

(d) časovnico za vaje in usposabljanja na področju VOI za okrepitev, potrditev in preskus načrta. Pridobljena spoznanja se dokumentirajo in vključijo v posodobitve načrta.

3. Nacionalna strategija VOI in nacionalni načrt za sodelovanje na področju VOI se sporočita Komisiji v enem mesecu po sprejetju.

Člen 6

Pristojni nacionalni organ za varnost omrežij in informacijskih sistemov

1. Vsaka država članica določi nacionalni organ, pristojen za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu „pristojni organ“).

2. Pristojni organi spremljajo uporabo te direktive na nacionalni ravni in prispevajo k njeni dosledni uporabi po vsej Uniji.

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.

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.

5. Pristojni organi se po potrebi posvetujejo in sodelujejo z ustreznimi nacionalnimi organi kazenskega pregona in organi za varstvo podatkov.

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.

Člen 7

Skupina za odzivanje na računalniške grožnje

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.

2. Države članice zagotovijo, da imajo CERT ustrezne tehnične, finančne in človeške vire za učinkovito izvajanje svojih nalog iz točke (2) Priloge I.

3. Države članice zagotovijo, da so CERT na nacionalni ravni podprte z varno in odporno komunikacijsko in informacijsko infrastrukturo, ki je združljiva in interoperabilna s sistemom za varno izmenjavo informacij iz člena 9.

4. Države članice Komisijo obvestijo o virih in pristojnostih ter o postopku obravnave incidentov v CERT.

5. CERT delujejo pod nadzorom pristojnega organa, ki redno pregleduje ustreznost njihovih virov, pristojnosti in učinkovitosti postopka obravnavanja incidentov.

POGLAVJE III

SODELOVANJE MED PRISTOJNIMI ORGANI

Člen 8

Mreža za sodelovanje

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.

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.

3. V okviru mreže za sodelovanje pristojni organi:

(a) širijo zgodnja opozorila o tveganjih in incidentih v skladu s členom 10;

(b) zagotavljajo usklajen odziv v skladu s členom 11;

(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;

(e) na zahtevo države članice ali Komisije skupaj ocenijo in razpravljajo o učinkovitosti 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 varstva podatkov, energije, prometa, bančništva, borze in zdravja;

(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 mednarodnih vajah na področju VOI.

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).

Člen 9

Sistem za varno izmenjavo informacij

1. Izmenjava občutljivih in zaupnih informacij v okviru mreže za sodelovanje se opravi prek varne infrastrukture.

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:

(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).

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).

Člen 10

Zgodnje opozarjanje

1. Pristojni organi 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;

(c) vplivajo ali lahko vplivajo 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.

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.

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.

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.

Člen 11

Usklajen odziv

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.

2. Različni ukrepi, sprejeti na nacionalni ravni kot posledica usklajenega odziva, se sporočijo mreži za sodelovanje.

Člen 12

Načrt za sodelovanje Unije na področju VOI

1. Komisija se pooblasti, da z izvedbenimi akti sprejme načrt za sodelovanje Unije na področju VOI. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 19(3).

2. Načrt za sodelovanje Unije na področju VOI določa:

(a) za namene člena 10:

– opredelitev oblike in postopkov za zbiranje in izmenjavo združljivih in primerljivih informacij o tveganjih in incidentih s strani pristojnih organov,

– opredelitev postopkov in meril za oceno tveganja in incidentov v mreži za sodelovanje.

(b) postopke, ki se upoštevajo pri usklajenem odzivanju v skladu s členom 11, vključno z opredelitvijo vlog in odgovornosti ter postopkov sodelovanja;

(c) časovnico za vaje in usposabljanja na področju VOI, da se načrt okrepi, potrdi in preskusi;

(d) program za prenos znanja med državami članicami v povezavi z gradnjo zmogljivosti in vzajemnim učenjem;

(e) program ozaveščanja in usposabljanja med državami članicami.

3. Načrt za sodelovanje Unije na področju VOI se sprejme najpozneje eno leto po začetku veljavnosti te direktive in se redno pregleduje.

Člen 13

Mednarodno 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. V takih sporazumih se upošteva potreba po zagotavljanju ustreznega varstva osebnih podatkov v mreži za sodelovanje.

POGLAVJE IV

VARNOST OMREŽIJ IN INFORMACIJSKIH SISTEMOV JAVNIH UPRAV IN TRŽNIH UDELEŽENCEV

Člen 14

Varnostne zahteve in priglasitev incidentov

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.

2. Države članice zagotovijo, da javne uprave in tržni udeleženci pristojnemu organu priglasijo incidente z bistvenim vplivom na varnost ključnih storitev, ki jih zagotavljajo.

3. Zahteve iz odstavkov 1 in 2 veljajo za vse tržne udeležence, ki zagotavljajo storitve v EU.

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.

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 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).

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[12].

Člen 15

Izvajanje in izvrševanje

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.

2. Države članice zagotovijo, da imajo pristojni organi pooblastila, da od tržnih udeležencev in javnih uprav zahtevajo, da:

   (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.

3. Države članice zagotovijo, da imajo pristojni organi pooblastila za izdajanje zavezujočih navodil za tržne udeležence in javne uprave.

4. Pristojni organi incidente, za katere sumijo, da so kriminalne narave, priglasijo organom kazenskega pregona.

5. Pristojni organi pri obravnavanju incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z organi za varstvo osebnih podatkov.

6. Države članice zagotovijo, da so obveznosti, ki se javnim upravam in tržnim udeležencem naložijo s tem poglavjem, lahko predmet sodne presoje.

Člen 16

Standardizacija

1. Za zagotovitev usklajenega izvajanja člena 14(1) države članice spodbujajo uporabo standardov in/ali specifikacij, ki se nanašajo na varnost omrežij in informacij.

[12] UL L 124, 20.5.2003, str. 36.

2. Komisija z izvedbenimi akti pripravi seznam standardov, navedenih v odstavku 1. Seznam objavi v Uradnem listu Evropske unije.

POGLAVJE V
KONČNE DOLOČBE

Člen 17

Sankcije

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.

2. Države članice zagotovijo, da so v primerih, ko ima varnostni incident posledice za varstvo osebnih podatkov, predvideni ukrepi skladni z ukrepi, določenimi v Uredbi Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov[13].

Člen 18

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.

Člen 19

Postopek v odboru

[13] SEC(2012) 72 final.

1. Komisiji pomaga odbor za varnost omrežij in informacij. Ta odbor je odbor po Uredbi (EU) št. 182/2011.

2. Pri sklicevanju na ta odstavek se uporablja člen 4 Uredbe (EU) št. 182/2011.

3. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Člen 20

Pregled

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.

Člen 21

Prenos

1. Države članice najpozneje do [leto in pol po sprejetju] sprejmejo in objavijo zakone in druge predpise, potrebne za uskladitev s to direktivo. Komisiji takoj sporočijo besedila navedenih predpisov.

   Navedene ukrepe uporabljajo od [leto in pol po sprejetju].

   Države članice se v sprejetih ukrepih sklicujejo na to direktivo ali pa sklic nanjo navedejo ob njihovi uradni objavi. Države članice določijo način sklicevanja.

2. Države članice sporočijo Komisiji besedilo temeljnih predpisov nacionalne zakonodaje, sprejetih na področju, ki ga ureja ta direktiva.

Člen 22

Začetek veljavnosti

Ta direktiva začne veljati [dvajseti] dan po objavi v *Uradnem listu Evropske unije*.

Člen 23

Naslovniki

Ta direktiva je naslovljena na države članice.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

PRILOGA I

Zahteve in naloge skupine za odzivanje na računalniške grožnje (CERT)

Zahteve in naloge CERT so ustrezno in jasno opredeljene ter podprte z nacionalno politiko in/ali zakonodajo. Vključujejo naslednje elemente:

(1) Zahteve za CERT:

(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.

(b) CERT izvajajo in upravljajo varnostne ukrepe, s čimer zagotovijo zaupnost, celovitost, razpoložljivost in verodostojnost informacij, ki jih prejmejo in obravnavajo.

(c) Uradi CERT in podporni informacijski sistemi se nahajajo na varnih krajih.

(d) Za nadaljnje spremljanje uspešnosti CERT in stalno izboljševanje se vzpostavi sistem za kakovost storitev upravljanja. Temelji na jasno opredeljenih meritvah, ki vključujejo formalne ravni storitev in ključne kazalce uspešnosti.

(e) Neprekinjeno poslovanje

- CERT so opremljene z ustreznim sistemom za upravljanje in usmerjanje zahtevkov, da se poenostavi njihova predaja,
- CERT imajo zadostno število strokovno usposobljenega osebja, da so razpoložljivi v vsakem trenutku,
- CERT temeljijo na infrastrukturi, ki ima zagotovljeno neprekinjeno delovanje. V ta namen se vzpostavijo podporni sistemi in nadomestni delovni prostor, da CERT lahko zagotovijo stalen dostop do komunikacijskih sredstev.

(2) Naloge CERT

(a) Naloge CERT vključujejo najmanj naslednje:

- spremljanje incidentov na nacionalni ravni,
- zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o tveganjih in incidentih ustreznim zainteresiranim stranem,
- odzivanje na incidente,
- opravljanje dinamičnih analiz tveganja in incidentov ter spremljanje razmer,
- krepitev ozaveščenosti širše javnosti o tveganjih, povezanih s spletnimi dejavnostmi,
- organiziranje kampanj o VOI;

(b) CERT sodelujejo z zasebnim sektorjem.

(c) Za lažje sodelovanje CERT spodbujajo sprejetje in uporabo skupnih ali standardiziranih praks za:

- postopke za obravnavanje incidentov in tveganj,
- sheme za klasifikacijo incidentov, tveganj in informacij,
- razvrščanje meritev,

– oblike izmenjave informacij o tveganjih, incidentih in dogovorih o poimenovanju sistemov.

PRILOGA II

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):

1. Energija

- Dobavitelji električne energije in plina
- Upravljavci sistema distribucije električne energije in/ali plina ter dobavitelji za končne uporabnike
- Upravljavci sistema za prenos zemeljskega plina, upravljavci skladišč in upravljavci obratov za UZP
- Upravljavci sistema za prenos električne energije
- Upravljavci cevovodov za prenos nafte in skladiščenja nafte
- Udeleženci na trgu elektrike in plina
- Upravljavci proizvodnje nafte in zemeljskega plina ter obratov za predelavo in rafiniranje

2. Promet

- Letalski prevozniki (tovorni in potniški zračni promet)
- Pomorski prevozniki (družbe za pomorski in obalni potniški promet in družbe za pomorski obalni tovorni promet)
- Železnice (upravitelji infrastrukture, integrirana podjetja in prevozniki v železniškem prometu)
- Letališča
- Pristanišča
- Izvajalci nadzora upravljanja prometa
- Pomožne logistične storitve: (a) skladiščenje in shranjevanje (b) ravnanje s tovorom in (c) druge spremljajoče prometne dejavnosti

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

5. Zdravstveni sektor: zdravstvenovarstvene ustanove (vključno z bolnišnicami in zasebnimi klinikami) ter drugi subjekti, ki zagotavljajo zdravstveno varstvo

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

1.2. Zadevna področja v strukturi ABM/ABB

1.3. Vrsta predloga/pobude

1.4. Cilji

1.5. Utemeljitev predloga/pobude

1.6. Trajanje ukrepa in finančnih posledic

1.7. Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

2.2. Upravljavski in kontrolni sistem

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2. Ocenjene posledica za odhodke

3.2.1. Povzetek ocenjenih posledic za odhodke

3.2.2. Ocenjene posledice za odobritve za poslovanje

3.2.3. Ocenjene posledice za odobritve za upravne zadeve

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

3.2.5. Udeležba tretjih oseb pri financiranju

3.3. Ocenjene posledice za prihodke

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke ravni varnosti omrežij in informacij v Uniji.

1.2. Zadevna področja v strukturi ABM/ABB[37]

- 09 – Komunikacijska omrežja, vsebine in tehnologija

1.3. Vrsta predloga/pobude

☒ Predlog/pobuda se nanaša na **nov ukrep**.

☐ Predlog/pobuda se nanaša na **nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[38].

☐ Predlog/pobuda se nanaša na **podaljšanje obstoječega ukrepa**.

☐ Predlog/pobuda se nanaša na **obstoječ ukrep, preusmerjen v nov ukrep**.

1.4. Cilji

1.4.1. Večletni strateški cilji Komisije, ki naj bi bili doseženi s predlogom/pobudo

Cilj predlagane direktive je zagotoviti visoko skupno raven varnosti omrežij in informacij po vsej EU.

1.4.2. Posebni cilji in zadevne dejavnosti v strukturi ABM/ABB

Predlog določa ukrepe za zagotavljanje visoke skupne ravni varnosti omrežij in informacijskih sistemov v Uniji.

Posebni cilji so:

1. Vzpostaviti minimalno raven VOI v državah članicah ter s tem povečati splošno raven pripravljenosti in odzivanja.

2. Izboljšati sodelovanje na področju VOI na ravni EU za učinkovito obravnavanje čezmejnih incidentov in groženj. Vzpostavljena bo infrastruktura za varno izmenjavo informacij, ki bo omogočila izmenjavo občutljivih in zaupnih informacij med pristojnimi organi.

3. Vzpostaviti kulturo obvladovanja tveganj ter izboljšati izmenjavo informacij med zasebnim in javnim sektorjem.

Zadevne dejavnosti v strukturi AMB/ABB

Direktiva se uporablja za subjekte (podjetja in organizacije, vključno z nekaterimi MSP) iz več sektorjev (energija, promet, kreditne institucije in borze, zdravstveno varstvo in ponudniki ključnih spletnih storitev) ter javne uprave. Ureja povezave z organi kazenskega pregona in organi za varstvo podatkov ter vidike VOI pri zunanjih odnosih.

- 09 – Komunikacijska omrežja, vsebine in tehnologija

- 02 – Podjetništvo

- 32 – Energetika

[37] ABM: upravljanje po dejavnostih – ABB: oblikovanje proračuna po dejavnostih.

[38] Po členu 49(6)(a) oz. (b) finančne uredbe.

- 06 – Mobilnost in promet

- 17 – Zdravje in varstvo potrošnikov

- 18 – Notranje zadeve

- 19 – Zunanji odnosi

- 33 – Pravosodje

- 12 – Notranji trg

1.4.3. Pričakovani rezultati in učinki

Navedite, kakšne posledice naj bi imel(-a) predlog/pobuda na upravičence/ciljne skupine.

Varstvo potrošnikov, podjetij in vlad EU pred incidenti, grožnjami in tveganji VOI bi se občutno izboljšalo.

Več podrobnosti je na voljo v oddelku 8.2 (Učinek možnosti 2 – regulativni pristop) delovnega dokumenta služb Komisije o oceni učinka, ki je priložen temu zakonodajnem predlogu.

1.4.4. Kazalniki rezultatov in učinkov

Navedite, s katerimi kazalniki se bo spremljalo izvajanje predloga/pobude.

Kazalniki za spremljanje in vrednotenje so opisani v oddelku 10 ocene učinka.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno

Vsaka država članica bi morala imeti:

– nacionalno strategijo VOI;

– načrt za sodelovanje na področju VOI;

– pristojni nacionalni organ za VOI ter

– skupino za odzivanje na računalniške grožnje (CERT).

Na ravni EU bi države članice morale sodelovati prek mreže za sodelovanje.

Javne uprave in ključni zasebni akterji bi morali izvajati ukrepe za obvladovanje tveganja VOI in pristojnim organom poročati o incidentih VOI z znatnim vplivom.

1.5.2. Dodana vrednost ukrepanja EU

Glede na čezmejno naravo VOI razlike v ustreznih zakonodajah in politikah ovirajo podjetja, ki delujejo v več državah, in svetovne ekonomije obsega. Neukrepanje na ravni EU bi povzročilo, da bi vsaka država članica ukrepala sama, pri čemer se ne bi upoštevala medsebojna odvisnost omrežij in informacijskih sistemov.

Navedene cilje se zato lažje doseže z ukrepanjem na ravni EU kot pa na ravni posameznih držav članic.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Predlog temelji na analizi, ki je pokazala, da so regulativne obveznosti potrebne za ustvarjanje enakih konkurenčnih pogojev in odpravo nekaterih zakonodajnih vrzeli. Povsem prostovoljni pristop je zagotovil sodelovanje samo manjšine držav članic z visoko stopnjo zmogljivosti.

1.5.4. Skladnost in možnosti sinergij z drugimi zadevnimi instrumenti

Predlog je v celoti skladen z digitalno agendo za Evropo in tako tudi s strategijo Evropa 2020. Prav tako je skladen z regulativnim okvirom za elektronske komunikacije, ki ga dopolnjuje, direktivo EU o evropski kritični infrastrukturi in direktivo EU o varstvu podatkov.

Predlog je bistven del sporočila Komisije ter visokega predstavnika Unije za zunanje zadeve in varnostno politiko o evropski strategiji za kibernetsko varnost, ki ga dopolnjuje.

1.6. Trajanje ukrepa in finančnih posledic

– ☐ Časovno omejen(-a) predlog/pobuda:

– ☐ trajanje predloga/pobude od [DD.MM.]LLLL do [DD.MM.]LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL.

– ☒ Časovno neomejen(-a) predlog/pobuda:

– obdobje prenosa se bo začelo takoj po sprejetju (predvidoma leta 2015) in bo trajalo 18 mesecev. Izvajanje direktive pa se bo začelo po sprejetju in bo vključevalo vzpostavitev varne infrastrukture, ki bo podpirala sodelovanje držav članic,

– sledi izvajanje predloga/pobude v celoti.

1.7. Načrtovani načini upravljanja[39]

– ☒ Neposredno centralizirano upravljanje – Komisija.

– ☒ Posredno centralizirano upravljanje – prenos izvajanja na:

– ☐ izvajalske agencije,

– ☒ organe, ki jih ustanovita Skupnosti[40],

– ☐ nacionalne javne organe/organe, ki zagotavljajo javne storitve,

– ☐ osebe, pooblaščene za izvajanje določenih ukrepov v skladu z naslovom V Pogodbe o Evropski uniji in opredeljene v zadevnem temeljnem aktu po členu 49 finančne uredbe.

– ☐ Deljeno upravljanje z državami članicami.

– ☐ Decentralizirano upravljanje s tretjimi državami.

– ☐ Skupno upravljanje z mednarodnimi organizacijami (tudi Evropsko vesoljsko agencijo).

Pri navedbi več kot enega načina upravljanja je treba to natančneje razložiti v oddelku „opombe“.

Opombe
Decentralizirana agencija ENISA, ki sta jih ustanovile Skupnosti, lahko državam članicam in Komisiji pomaga pri izvajanju te direktive na podlagi svojega mandata in prerazporeditve sredstev, predvidenih za to agencijo v okviru večletnega finančnega okvira za obdobje 2014–2020.

[39] Pojasnitve načinov upravljanja in sklicevanje na finančno uredbo so na voljo na spletišču BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[40] Organi iz člena 185 finančne uredbe.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo redno pregledovala delovanje te direktive ter o tem poročala Evropskemu parlamentu in Svetu.

Komisija bo prav tako ocenila pravilen prenos direktive v državah članicah.

Predlog uredbe IPE določa tudi ocenjevanje načinov izvajanja projektov ter učinka njihovega izvajanja, da se oceni, ali so bili doseženi cilji, vključno s cilji varstva okolja.

2.2. Upravljavski in kontrolni sistem

2.2.1. Ugotovljena tveganja

– zamude pri izvajanju projekta (gradnja varne infrastrukture)

2.2.2. Načrtovani načini kontrole

Sporazumi in sklepi o izvajanju ukrepov v okviru IPE bodo zagotovili nadzor in finančno kontrolo s strani Komisije ali katerega koli predstavnika, ki ga pooblasti Komisija, revizije Računskega sodišča in preglede na kraju samem, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF).

2.2.3. Stroški in koristi kontrol ter pričakovana stopnja neskladnosti

Predhodne in naknadne kontrole, temelječe na tveganju, in možnost pregleda na kraju samem bodo zagotovile, da bodo stroški kontrole razumni.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe.

Komisija sprejme ustrezne ukrepe, s katerimi zagotovi, da so pri izvajanju ukrepov, ki se financirajo na podlagi tega sklepa, finančni interesi Evropske unije zaščiteni z izvajanjem preventivnih ukrepov proti goljufijam, korupciji in drugemu protipravnemu ravnanju ter z učinkovitim preverjanjem, ob odkritju nepravilnosti pa z izterjavo neupravičeno izplačanih zneskov ter po potrebi z učinkovitimi, sorazmernimi in odvračilnimi kaznimi.

Komisija ali njeni predstavniki in Računsko sodišče lahko opravijo preglede na podlagi dokumentacije in na kraju samem pri vseh prejemnikih nepovratnih sredstev, izvajalcih in podizvajalcih, ki so prejeli sredstva Unije na podlagi tega sklepa.

Evropski urad za boj proti goljufijam (urad OLAF) lahko opravi preglede in inšpekcije na kraju samem pri gospodarskih subjektih, ki jih neposredno ali posredno zadeva takšno financiranje, v skladu s postopki iz Uredbe Sveta (Euratom, ES) št. 2185/96, da bi ugotovil, ali je v povezavi s sporazumom ali sklepom o nepovratnih sredstvih ali pogodbo o financiranju s strani Unije prišlo do goljufije, korupcije ali drugega protipravnega ravnanja, ki škodi finančnim interesom Unije.

Ne glede na zgornje odstavke se v sporazumih o sodelovanju s tretjimi državami in mednarodnimi organizacijami, sporazumih o nepovratnih sredstvih, sklepih o nepovratnih sredstvih in pogodbah, ki izhajajo iz izvajanja te uredbe, Komisija,

Računsko sodišče in urad OLAF izrecno pooblastijo za opravljanje takšnih revizij ter pregledov in inšpekcij na kraju samem.

IPE določa, da morajo pogodbe o nepovratnih sredstvih in naročila temeljiti na standardnih modelih, ki določajo splošno veljavne ukrepe proti goljufijam.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe odhodkovne proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka [poimenovanje……..…….]	dif./ nedif. (41)	držav Efte[42]	držav kandidatk[43]	tretjih držav	po členu 18(1)(aa) finančne uredbe
	09 03 02 spodbujanje medsebojnega povezovanja in interoperabilnosti nacionalnih javnih storitev v spletu in dostopa do takih omrežij	dif.	NE	NE	NE	NE

- Zahtevane nove proračunske vrstice (ni relevantno)

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka [poimenovanje……..…….]	dif./ nedif.	držav Efte	držav kandidatk	tretjih držav	po členu 18(1)(aa) finančne uredbe
	[XX YY YY YY]		DA/NE	DA/NE	DA/NE	DA/NE

41 Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.

42 EFTA: Evropsko združenje za prosto trgovino.

43 Države kandidatke in po potrebi potencialne države kandidatke Zahodnega Balkana.

3.2. Ocenjene posledice za odhodke

3.2.1. Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira:	1	Pametna in vključujoča rast

GD za: <…….>			2015* [44]	Leto **2016**	Leto **2017**	Leto **2018**	Naslednja leta (2019–2021) in naprej			**SKUPAJ**
• Odobritve za poslovanje										
09 03 02	obveznosti	(1)	1,250**	0,000						**1,250**
	plačila	(2)	0,750	0,250	0,250					**1,250**
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov[45]			**0,000**							**0,000**
Številka proračunske vrstice		(3)	**0,000**							**0,000**
Odobritve za GD za <…….> SKUPAJ	obveznosti	=1+1a +3	1,250	0,000						**1,250**
	plačila	=2+2a +3	0,750	0,250	0,250					**1,250**

• Odobritve za poslovanje SKUPAJ	obveznosti	(4)	1,250	0,000						**1,250**
	plačila	(5)	0,750	0,250	0,250					**1,250**
• Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)	**0,000**							

[44] Leto N je leto začetka izvajanja predloga/pobude.

[45] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

Odobritve iz RAZDELKA 1 večletnega finančnega okvira SKUPAJ	obveznosti	=4+ 6	1,250	0,000						**1,250**
	plačila	=5+ 6	0,750	0,250	0,250					**1,250**

* Natančna časovnica bo odvisna od datuma, na katerega bo zakonodajni organ sprejel predlog (tj. če bo direktiva odobrena leta 2014, se bo prilagoditev obstoječe infrastrukture začela leta 2015, sicer pa eno leto pozneje).

** Če se države članice odločijo, da uporabijo obstoječo infrastrukturo in plačajo enkratne stroške prilagoditve iz proračuna EU, kakor je pojasnjeno v točkah 1.4.3 in 1.7, so stroški za prilagoditev mreže, da bo lahko podpirala sodelovanje držav članic v skladu s Poglavjem II Direktive (zgodnje opozarjanje, usklajeno odzivanje itd.) ocenjeni na 1 250 000 EUR. Ta znesek je nekoliko večji kot tisti, naveden v oceni učinka („približno 1 milijon EUR“), saj temelji na bolj natančni oceni elementov, potrebnih za takšno infrastrukturo. Potrebni elementi in z njimi povezani stroški temeljijo na oceni JRC, ki je bila opravljena na podlagi izkušenj pri razvijanju podobnih sistemov na drugih področjih, kot je javno zdravje, in bi vključevali: sistem za hitro opozarjanje in obveščanje na področju VOI (275 000 EUR); platformo za izmenjavo informacij (400 000 EUR); sistem za zgodnje opozarjanje in odzivanje (275 000 EUR); situacijska soba (300 000 EUR), skupaj 1 250 000 EUR. Podrobnejši izvedbeni načrt bo po pričakovanjih pripravljen v prihodnji študiji izvedljivosti v okviru posebne pogodbe SMART 2012/0010: „Študija izvedljivosti in pripravljalne dejavnosti za vzpostavitev evropskega sistema za zgodnje opozarjanje in odzivanje na kibernetske napade in prekinitve“.

Če ima predlog/pobuda posledice za več razdelkov:

• Odobritve za poslovanje SKUPAJ	obveznosti	(4)	0,000	0,000						
	plačila	(5)	0,000	0,000						
• Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)	**0,000**	**0,000**						
Odobritve iz RAZDELKOV od 1 do 4 večletnega finančnega okvira SKUPAJ (referenčni znesek)	obveznosti	=4+ 6	1,250	0,000						1,250
	plačila	=5+ 6	0,750	0,250	0,250					1,250

Razdelek večletnega finančnega okvira	**5**	„Upravni odhodki“

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2015**	Leto **2016**	Leto **2017**	Leto **2018**	Naslednja leta (2019–2021) in naprej			**SKUPAJ**
GD za komunikacijska omrežja, vsebine in tehnologijo									
• Človeški viri		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Drugi upravni odhodki		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
GD za komunikacijska omrežja, vsebine in tehnologijo SKUPAJ	odobritve	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Odobritve iz RAZDELKA 5 večletnega finančnega okvira SKUPAJ	(obveznosti skupaj = plačila skupaj)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2015**[46]	Leto **2016**	Leto **2017**	Leto **2018**	Naslednja leta (2019–2021) in naprej			**SKUPAJ**
Odobritve iz RAZDELKOV od 1 do 5 večletnega finančnega okvira SKUPAJ	obveznosti	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	plačila	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Leto N je leto začetka izvajanja predloga/pobude.

3.2.2. Ocenjene posledice za odobritve za poslovanje

– ☐ Za predlog/pobudo niso potrebne odobritve za poslovanje.

– ☑ Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

– odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno)

Cilji in realizacije ⇩			Leto **2015***		Leto **2016**		Leto **2017**		Leto **2018**		Naslednja leta (2019–2021) in naprej						**SKUPAJ**	
	REALIZACIJE																	
	vrsta realizacije[47]	Povprečni stroški realizacije	število realizacij	stroški	število realizacij	stroški	število realizacij	stroški	število realizacij	stroški	število realizacij	stroški	Število realizacij	stroški	Število realizacij	stroški	število realizacij skupaj	stroški skupaj
POSAMEZNI CILJ št. 2[48] Infrastruktura za varno izmenjavo informacij																		
– realizacija	Prilagoditev infrastrukture																	
Seštevek za posamezni cilj št. 2			1	1,250**													1	1,250
STROŠKI SKUPAJ				1,250														1,250

47 Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

48 Kakor je opisan v oddelku 1.4.2. „Posamezni cilji …“.

* Natančna časovnica bo odvisna od datuma, na katerega bo zakonodajni organ sprejel predlog (tj. če bo direktiva odobrena leta 2014, se bo prilagoditev obstoječe infrastrukture začela leta 2015, sicer pa eno leto pozneje).

** Glej točko 3.2.1.

3.2.3. Ocenjene posledice za odobritve za upravne zadeve

3.2.3.1. Povzetek

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☑ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto **2015**[49]	Leto **2016**	Leto **2017**	Leto **2018**	Naslednja leta (2019–2021) in naprej			**SKUPAJ**
RAZDELEK 5 večletnega finančnega okvira								
Človeški viri	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Drugi upravni odhodki	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Seštevek za RAZDELEK 5 večletnega finančnega okvira	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Odobritve zunaj RAZDELKA 5[50] **večletnega finančnega okvira**								
Človeški viri	0,000	0,000						**0,000**
Drugi upravni odhodki								
Seštevek za odobritve zunaj RAZDELKA 5 večletnega finančnega okvira	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

SKUPAJ	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Zahtevane upravne odobritve se krijejo z odobritvami GD za komunikacijska omrežja, vsebine in tehnologijo, že dodeljenimi za upravljanje ukrepa in/ali prerazporejenimi znotraj GD za komunikacijska omrežja, vsebine in tehnologijo, po potrebi dopolnjenimi z dodatnimi viri, ki se lahko GD, pristojnemu za upravljanje, dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

49 Leto N je leto začetka izvajanja predloga/pobude.

50 Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

Evropska agencija za varnost omrežij (ENISA) bi lahko pomagala državam članicam in Komisiji pri izvajanju te direktive na podlagi svojega mandata in s prerazporeditvijo sredstev iz večletnega finančnega okvira za obdobje 2014–2020 za to agencijo, tj, brez dodatnih dodeljenih proračunskih ali človeških virov.

3.2.3.2. Ocenjene potrebe po človeških virih

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– ☑ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

Načeloma dodatna delovna sila ne bi bila potrebna. Potrebe po človeških virih bodo zelo omejene in se bodo krile z osebjem GD, ki mu je že zdaj zaupano upravljanje ukrepa.

ocena, izražena v celih številkah (ali na največ eno decimalno mesto natančno)

	Leto **2015**	Leto **2016**	Leto 2017	Leto 2018	Naslednja leta (2019–2021) in naprej		
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)							
09 01 01 01 (sedež ali predstavništva Komisije)	4	4	4	4	4	4	4
XX 01 01 02 (delegacije)							
XX 01 05 01 (posredne raziskave)							
10 01 05 01 (neposredne raziskave)							
• Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[51]							
09 01 02 01 (PU, ZU, NNS iz splošnih sredstev)	1	1	1	1	1	1	1
XX 01 02 02 (PU, ZU, MSD, LU in NNS na delegacijah)							
XX 01 04 yy[52] – na sedežu[53]							
XX 01 04 yy[52] – na delegacijah							
XX 01 05 02 (PU, ZU, NNS za posredne raziskave)							
10 01 05 02 (PU, ZU, NNS za neposredne raziskave)							
Druge proračunske vrstice (navedite)							
SKUPAJ	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX je zadevno področje ali naslov.

Potrebe po človeških virih se krijejo z osebjem GD, že dodeljenim za upravljanje tega ukrepa in/ali prerazporejenim znotraj GD, po potrebi z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

Evropska agencija za varnost omrežij (ENISA) bi lahko pomagala državam članicam in Komisiji pri izvajanju te direktive na podlagi trenutnega mandata in s prerazporeditvijo sredstev iz večletnega finančnega okvira za obdobje 2014–2020 za to agencijo, tj, brez dodatnih dodeljenih proračunskih ali človeških virov.

[51] PU = pogodbeni uslužbenec; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak.

[52] V okviru zgornje meje za zunanje sodelavce iz odobritev za poslovanje (prej vrstice BA).

[53] Zlasti za strukturna sklada, Evropski kmetijski sklad za razvoj podeželja (EKSRP) in Evropski sklad za ribištvo (ESR).

Opis nalog:

Uradniki in začasni uslužbenci	– priprava delegiranih aktov v skladu s členom 14 (3) – priprava izvedbenih aktov v skladu s členi 8, 9 (2), 12, 14(5) in 16 – prispevek k sodelovanju prek mreže tako na politični kot operativni ravni – sodelovanje pri mednarodnih razpravah in morebitnemu sklepanju mednarodnih sporazumov
Zunanji sodelavci	– po potrebi podpora vsem zgoraj navedenim nalogam

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

– ☑ Predlog/pobuda je v skladu z veljavnim večletnim finančnim okvirom.

– ☐ Za predlog/pobudo bo potrebna sprememba zadevnega razdelka večletnega finančnega okvira.

Ocenjene finančne posledice predloga za odhodke iz poslovanja predloga bodo nastale, če se države članice odločijo za prilagoditev obstoječe infrastrukture in za to v okviru večletnega finančnega okvira za obdobje 2014–2020 pooblastijo Komisijo. Povezani enkratni stroški bi bili kriti v okviru IPE, pod pogojem, da je na voljo dovolj sredstev. Druga možnost je, da si države članice delijo stroške prilagoditve infrastrukture ali stroške vzpostavitve nove infrastrukture.

– ☐ Za predlog/pobudo je potrebna uporaba instrumenta prilagodljivosti ali sprememba večletnega finančnega okvira[54].

Ni relevantno.

3.2.5. Udeležba tretjih oseb pri financiranju

– V predlogu/pobudi ni načrtovano sofinanciranje tretjih oseb.

3.3. Ocenjeni učinek na prihodke

– ☑ Predlog/pobuda nima finančnih posledic za prihodke.

[54] Glej točki 19 in 24 Medinstitucionalnega sporazuma.